Exam Questions PCCSE

Prisma Certified Cloud Security Engineer

https://www.2passeasy.com/dumps/PCCSE/

NEW QUESTION 1
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 2
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 3
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 4
Which port should a security team use to pull data from Console's API?

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

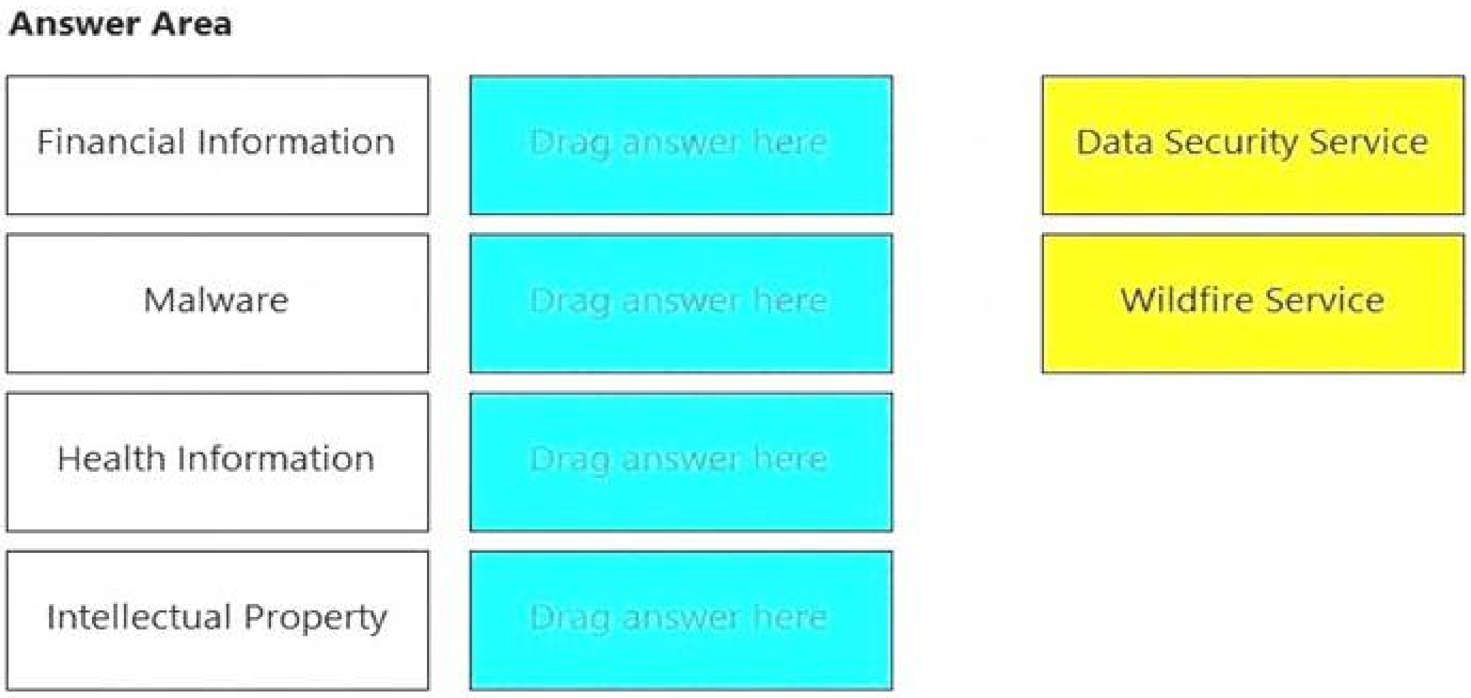
Answer: D

NEW QUESTION 5
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 6
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

Malware | Drag answer here

Health Information | Drag answer here

Intellectual Property | Drag answer here

Data Security Service

Wildfire Service

A. Mastered
B. Not Mastered

Answer: A

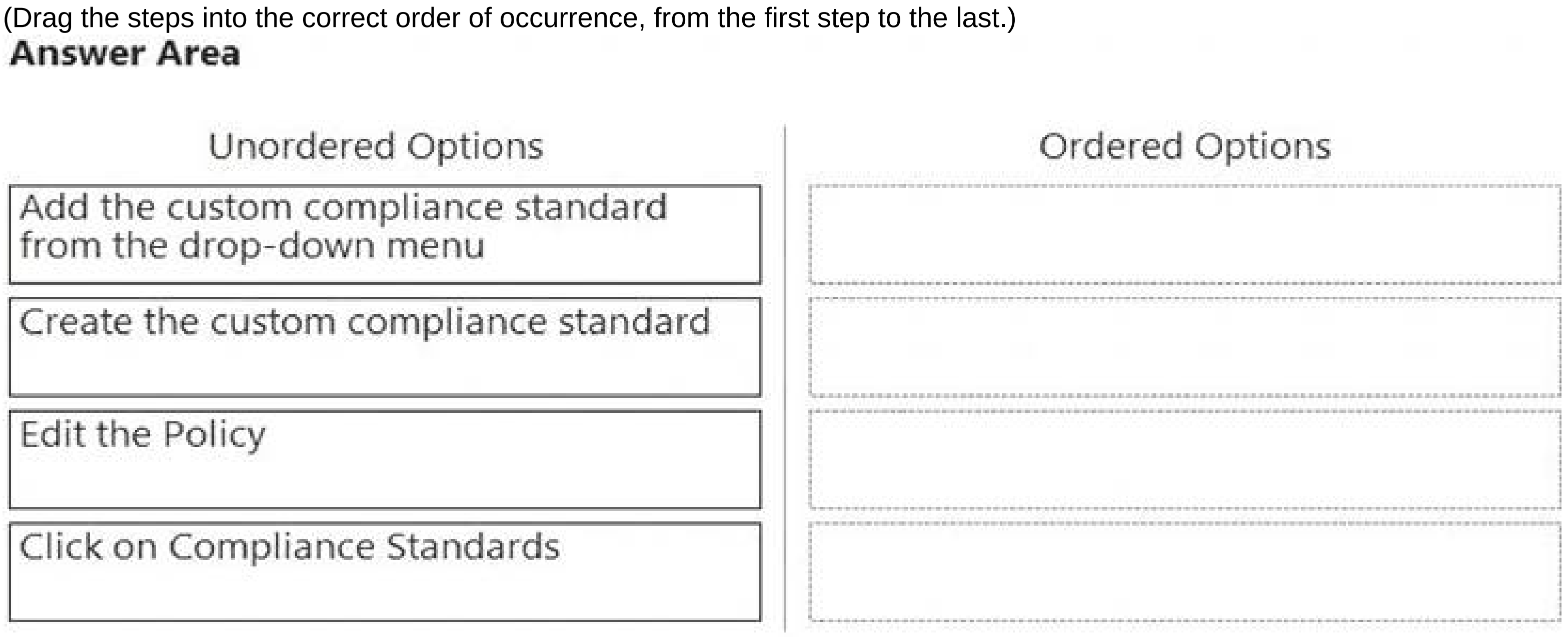
Explanation:
Diagram Description automatically generated

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
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

Add the custom compliance standard from the drop-down menu

Create the custom compliance standard

Edit the Policy

Click on Compliance Standards

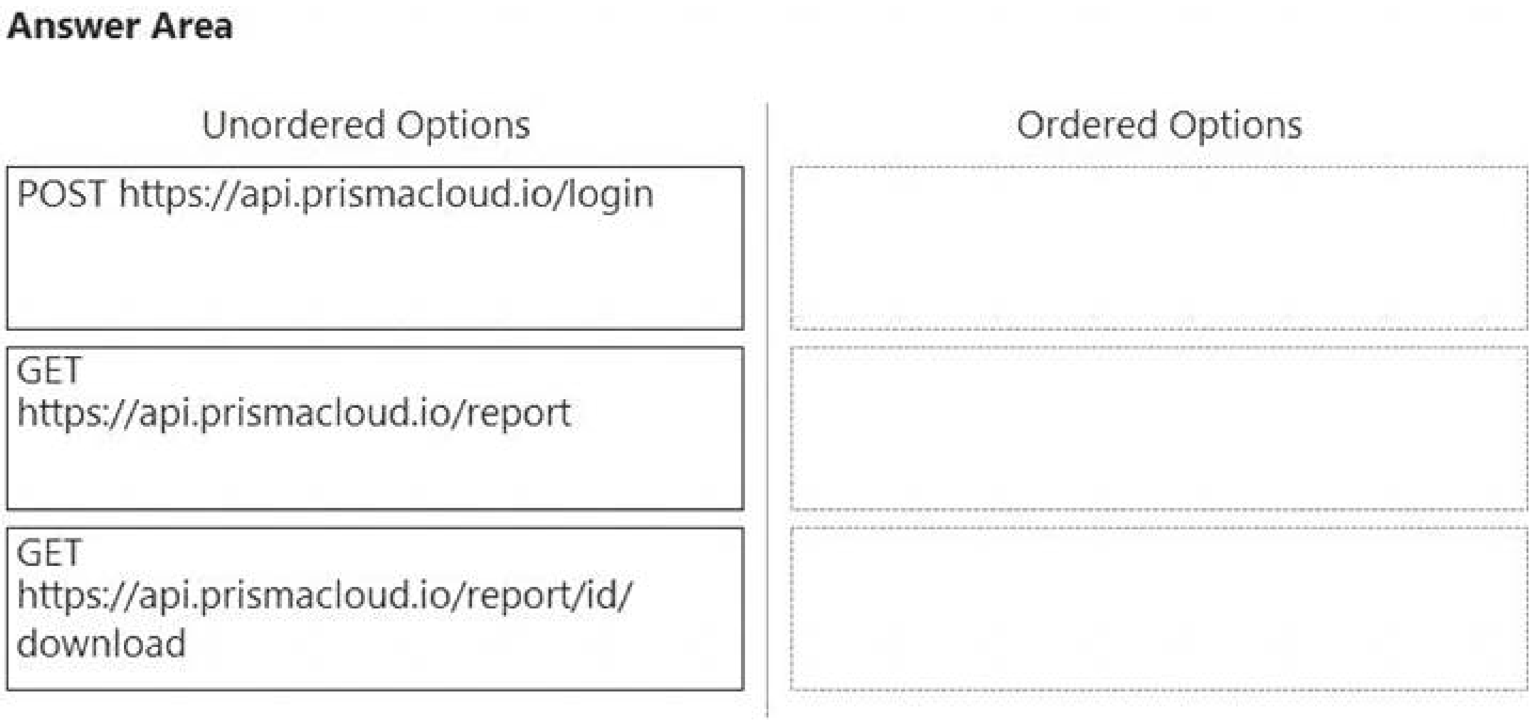
Ordered Options

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Diagram Description automatically generated

NEW QUESTION 9
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

Unordered Options

POST https://api.prismacloud.io/login

GET https://api.prismacloud.io/report

GET https://api.prismacloud.io/report/id/download

Ordered Options

A. Mastered
B. Not Mastered

Answer: A

Explanation:
A picture containing graphical user interface Description automatically generated

NEW QUESTION 10
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 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

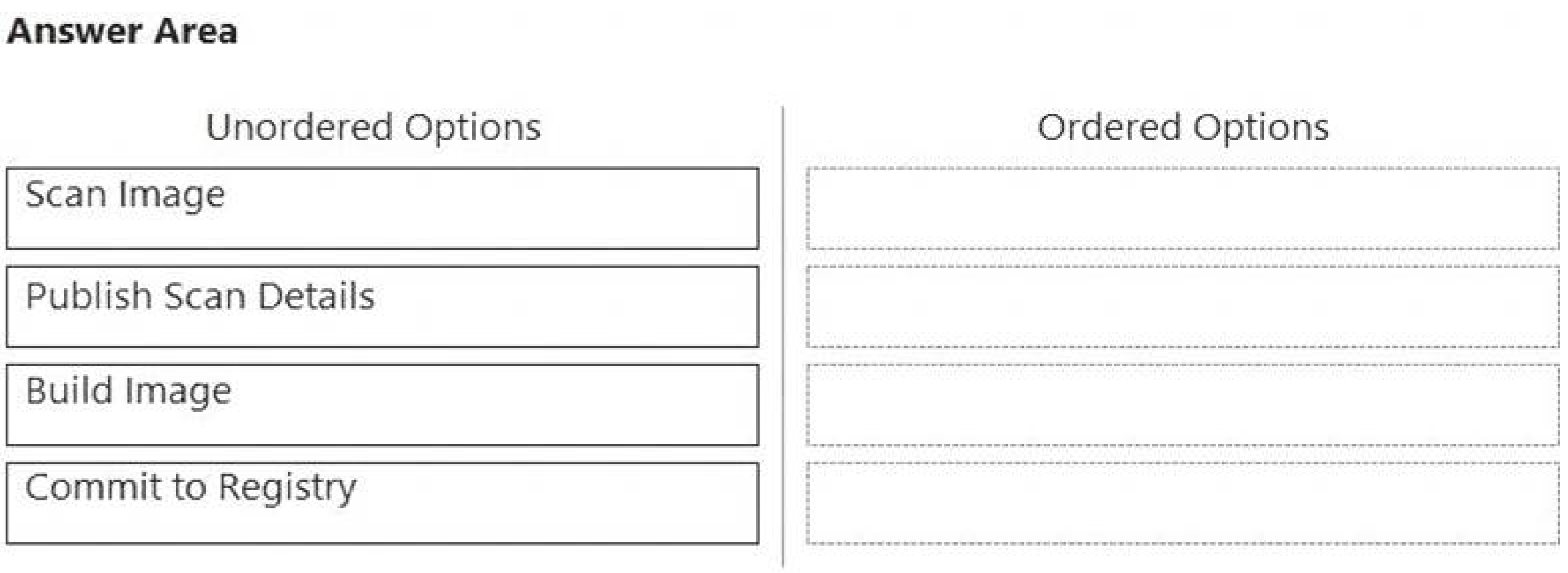
Answer: A

NEW QUESTION 12
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 16
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 17
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 21
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 24
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 “prevent”.
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 “Explicitly allowed inbound IP sources” to the IP address of the pod.

Answer: A

NEW QUESTION 26
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 27
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 30
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 32
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 36
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.

Answer: AD

NEW QUESTION 37
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 38
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 cluste
B. A onebox deployment should be used.
C. Download and extract the release tarballEnsure that each node has its own storage for Console data Create the Console task definition Deploy the task definition
D. Download and extract release tarball Download task from AWS Create the Console task definition Deploy the task definition
E. Download and extract the release tarballCreate an EFS file system and mount to each node in the cluster Create the Console task definition Deploy the task definition

Answer: D

NEW QUESTION 39
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 44
Which options show the steps required to upgrade Console when using projects?

A. Upgrade all Supervisor Consoles Upgrade Central Console
B. Upgrade Central ConsoleUpgrade Central Console Defenders
C. Upgrade Defender Upgrade Central Console Upgrade Supervisor Consoles
D. Upgrade Central Console Upgrade all Supervisor Consoles

Answer: A

NEW QUESTION 47
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 49
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 50
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 52
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 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 59
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 61
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 64
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.

Answer: B

NEW QUESTION 66
......