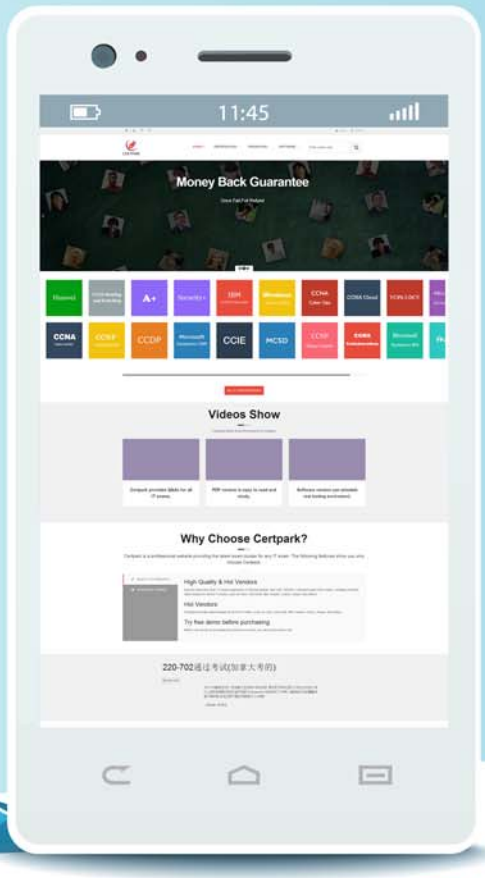
CERTPARK

QUESTION & ANSWER

CERTPARK.COM

Accurate Study Guides,
High Passing Rate!
provides update
free of charge
in one year!



https://www.certpark.com

Exam : **PCCSE**

Title : Prisma Certified Cloud Security Engineer

Version : DEMO

1.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
Explanation:
Reference: https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/compliance/manage_compliance.html
In the context of Prisma Cloud by Palo Alto Networks, the correct navigation to identify alerted compliance checks set by default is under the "Defend" section, specifically at "Defend > Compliance." This section is designed to allow users to configure and manage compliance policies and rules, monitor compliance statuses, and review alerts related to compliance violations. The "Defend" section is tailored for setting up defenses, including compliance standards, against potential security risks within the cloud environment, making it the logical location for managing and reviewing compliance-related alerts and settings.

2.Which container scan is constructed correctly?
A. twistcli images scan -u api -p api --address https://us-west1.cloud.twistlock.com/us-3-123456789 - -container myimage/latest
B. twistcli images scan --docker-address https://us-west1.cloud.twistlock.com/us-3-123456789 myimage/latest
C. twistcli images scan -u api -p api --address https://us-west1.cloud.twistlock.com/us-3-123456789 - -details myimage/latest
D. twistcli images scan -u api -p api --docker-address https://us-west1.cloud.twistlock.com/us-3-123456789 myimage/latest
Answer: C
Explanation:
The correct construction for a container scan using the TwistCLI tool provided by Prisma Cloud (formerly Twistlock) is shown in option
C. This command uses the TwistCLI tool to scan a container image, specifying the necessary authentication credentials (username and password with '-u' and '-p' flags), the address of the Prisma Cloud instance (with the '--address' flag), and the image to be scanned (in this case, 'myimage/latest'). The inclusion of the '--details' flag is a common practice to obtain detailed scan results, which is crucial for in-depth analysis and remediation efforts. This command structure aligns with the standard usage of TwistCLI for image scanning purposes, as documented in Prisma Cloud's official resources and guides.

3.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: D
Explanation:
Reference tech docs: https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/continuous_integration/set_policy_ci_plugins.html
Vulnerability rules that target the build tool can allow specific vulnerabilities by creating an exception and setting the effect to 'ignore'. Block them by creating an exception and setting hte effect to 'fail'. For example, you could create a vulnerability rule that explicitly allows CVE-2018-1234 to suppress warnings in the scan results.
To fail CI jobs based on a specific CVE contained within an image, the development team should configure the policy within Prisma Cloud's Console, specifically within the Continuous Integration (CI) policy settings. By setting a specific CVE exception in the CI policy, the team can define criteria that will cause the CI process to fail if the specified CVE is detected in the scanned image. This approach allows for granular control over the build process, ensuring that images with known vulnerabilities are not promoted through the CI/CD pipeline, thereby maintaining the security posture of the deployed applications. This method is in line with best practices for integrating security into the CI/CD process, allowing for automated enforcement of security standards directly within the development pipeline.

4.Which three types of classifications are available in the Data Security module? (Choose three.)
A. Personally identifiable information
B. Malicious IP
C. Compliance standard
D. Financial information
E. Malware
Answer: ACD
Explanation:
https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/prisma-cloud-data-security.html
In the Data Security module of Prisma Cloud, the classifications available focus on the types of sensitive data that need protection. These classifications include Personally Identifiable Information (PII), which involves data that can be used on its own or with other information to identify, contact, or locate a single person. Compliance standards pertain to data that must be protected to meet specific regulatory requirements, such as GDPR, HIPAA, or PCI-DSS. Financial information classification is concerned with data related to financial transactions, accounts, and credit card numbers, which are critical to secure due to their sensitive nature. These classifications are integral to data security strategies, ensuring that sensitive information is adequately protected according to its nature and the regulatory requirements governing it.

5.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

Explanation:

To terminate any Container from the image "topSecret:latest" when a process named "ransomWare" is executed, the administrator should create a new runtime policy in Prisma Cloud Compute specifically targeting the container in question. By adding the "ransomWare" process to the denied process list within this policy and setting the action to "prevent," Prisma Cloud Compute will actively
monitor for the execution of the specified process within the targeted container and take preventive action to terminate the container if the process is detected. This approach allows for precise, targeted security measures that address specific threats identified by the organization, thereby enhancing the overall security posture and protecting sensitive workloads from potential compromise.