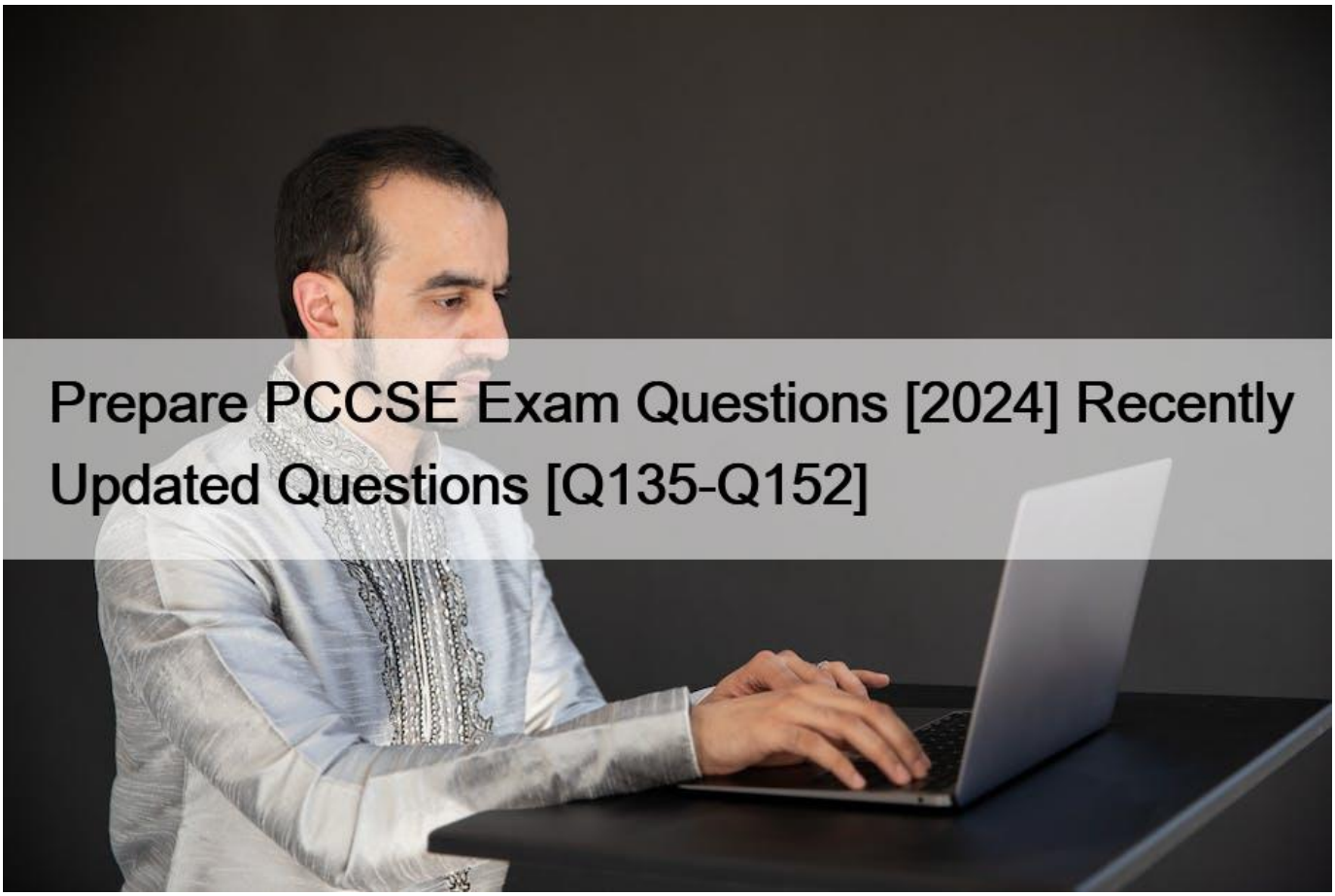
Prepare PCCSE Exam Questions [2024 Recently Updated Questions [Q135-Q152



Prepare PCCSE Exam Questions [2024 Recently Updated Questions Give push to your success with PCCSE exam questions

To be eligible to take the PCCSE exam, candidates must have at least one year of experience in cloud security and hold a current certification in either the Palo Alto Networks Certified Network Security Engineer (PCNSE) or the Palo Alto Networks Certified Prisma Access Security Engineer (PCSSE) exam. The PCCSE exam is a proctored exam that can be taken online from anywhere in the world. PCCSE exam consists of 60 multiple-choice questions and must be completed within 120 minutes.

NEW QUESTION 135

The security auditors need to ensure that given compliance checks are being run on the host. Which option is a valid host compliance policy?

* Ensure compliant Docker daemon configuration
* Ensure functions are not overly permissive.
* Ensure images are created with a non-root user
* Ensure host devices are not directly exposed to containers.

NEW QUESTION 136

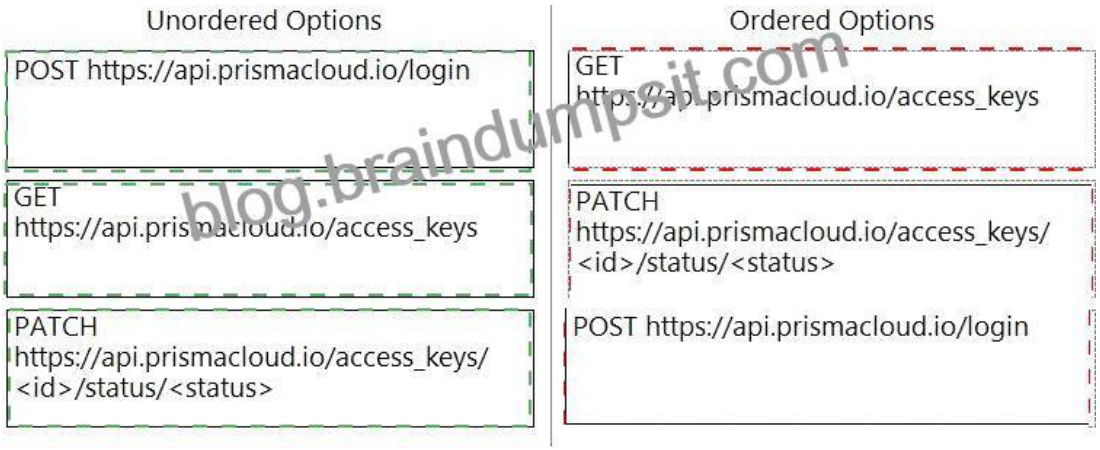
An administrator needs to write a script that automatically deactivates access keys that have not been used for

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

Answer Area



Explanation

A picture containing graphical user interface Description automatically generated

Answer Area

NEW QUESTION 137

Which two actions are required in order to use the automated method within Amazon Web Services (AWS) Cloud to streamline the process of using remediation in the identity and access management (IAM) module?

(Choose two.)
* Install boto3 & requests library.
* Configure IAM Azure remediation script.
* Integrate with Azure Service Bus.
* Configure IAM AWS remediation script.

To utilize the automated method for remediation within the Amazon Web Services (AWS) Cloud, specifically for the Identity and Access Management (IAM) module, two critical actions are required: installing the boto3 and requests libraries, and configuring the IAM AWS remediation script.

The boto3 library is AWS’s SDK for Python, allowing Python developers to write software that makes use of services like Amazon S3 and Amazon EC2. The requests library is a Python HTTP library designed for human beings, enabling easy interaction with HTTP services. Together, these libraries are foundational for scripting AWS services, including automating remediation tasks within IAM.

Configuring the IAM AWS remediation script is the second critical step. This script is tailored to interact with AWS IAM to automate the remediation of identified security issues, such as excessive permissions, unused IAM roles, or improperly configured policies. The script uses the boto3 library to communicate with AWS services, applying the necessary changes to align IAM configurations with security best practices.

These actions are essential for leveraging automation to enhance IAM security within AWS, ensuring that IAM configurations adhere to the principle of least privilege and other security best practices. This approach aligns with Prisma Cloud’s capabilities and recommendations for cloud security, emphasizing the importance of automation in maintaining a robust security posture, as discussed in resources like the “Prisma Cloud Visibility and Control Qualification Guide” and the “Guide to Cloud Security Posture Management Tools.” References:

* “Prisma Cloud Visibility and Control Qualification Guide” highlights the significance of automated security controls and remediation within cloud environments, supporting the use of scripts and libraries for IAM remediation in AWS.

* “Guide to Cloud Security Posture Management Tools” emphasizes the importance of automation in cloud security, particularly for managing and remediating IAM configurations to ensure compliance and minimize risks.

NEW QUESTION 138

In which two ways can Prisma Cloud images be retrieved in Prisma Cloud Compute Self-Hosted Edition?

(Choose two.)
* Pull the images from the Prisma Cloud registry without any authentication.
* Authenticate with Prisma Cloud registry, and then pull the images from the Prisma Cloud registry.
* Retrieve Prisma Cloud images using URL auth by embedding an access token.
* Download Prisma Cloud images from github.paloaltonetworks.com.

In Prisma Cloud Compute Self-Hosted Edition, images can be retrieved by first authenticating with the Prisma Cloud registry and then pulling the images from the Prisma Cloud registry. This process ensures secure access to Prisma Cloud images, as authentication is required to access the registry. By using authentication, Prisma Cloud ensures that only authorized users can retrieve and deploy Prisma Cloud images, maintaining the security and integrity of the deployment.

NEW QUESTION 139

A customer has a requirement to restrict any container from resolving the name www.evil-url.com.

How should the administrator configure Prisma Cloud Compute to satisfy this requirement?
* Choose “copy into rule” for any Container, set www.evil-url.com as a blocklisted DNS name in the Container policy and set the policy effect to alert.
* Set www.evil-url.com as a blocklisted DNS name in the default Container runtime policy, and set the effect to block.
* Choose “copy into rule” for any Container, set www.evil-url.com as a blocklisted DNS name, and set the effect to prevent.
* Set www.evil-url.com as a blocklisted DNS name in the default Container policy and set the effect to prevent.

To restrict any container from resolving the name www.evil-url.com, the administrator should set www.evil-url.com as a blocklisted DNS name in the default Container policy and set the effect to prevent.

This configuration in Prisma Cloud, or similar CSPM tools, ensures that any attempt to resolve the specified blocklisted DNS name within any container will be prevented, thus enhancing security by proactively blocking potential communication with known malicious domains.

Reference to this feature can be found in the documentation of CSPM tools that offer runtime protection for containers. These tools allow administrators to define security policies that can include DNS-based controls to prevent containers from accessing known malicious or undesirable URLs, thereby preventing potential data exfiltration, malware communication, or other security threats

NEW QUESTION 140

What is the behavior of Defenders when the Console is unreachable during upgrades?
* Defenders will fail open until the web-socket can be reestablished.
* Defenders will fail closed until the web-socket can be re-established
* Defenders continue to alert, but not enforce, using the policies and settings most recently cached before upgrading the Console.
* Defenders continue to alert and enforce using the policies and settings most recently cached before upgrading the Console.

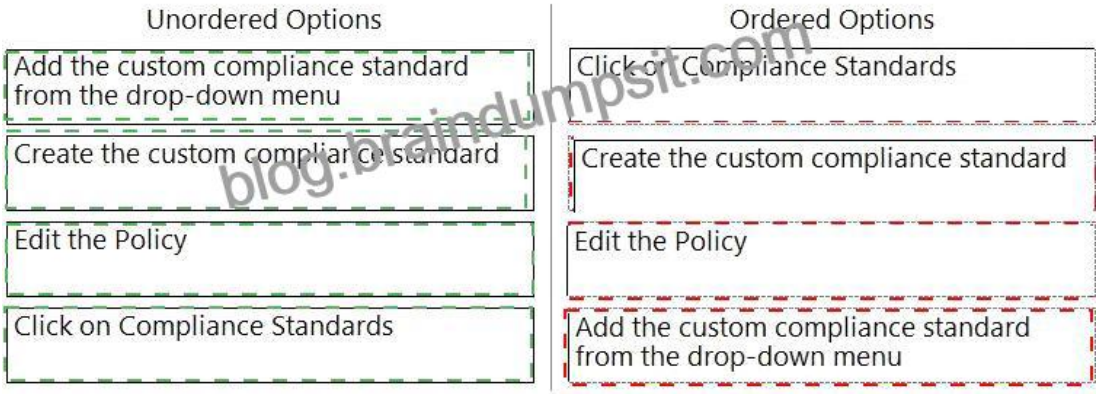
NEW QUESTION 141

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

Answer Area



Explanation:

1. click on compliance standard.

2. add custom compliance standard.

3. edit policies.

4. add compliance standard from drop-down menu

https://docs.prismacloudcompute.com/docs/enterprise_edition/compliance/custom_compliance_checks.html#cre The process of mapping a policy to a custom compliance standard in a security platform like Prisma Cloud by Palo Alto Networks involves several specific steps. Firstly, one must access the compliance standards, which is typically done by clicking on the “Compliance Standards” section within the platform’s interface. This is where all standards, including custom and predefined ones, are listed.

Next, if the custom compliance standard does not already exist, it must be created. This step involves defining the criteria and controls that make up the standard, tailored to the organization’s specific requirements.

Once the custom compliance standard is in place, the policy in question needs to be edited. This editing process would involve configuring the policy to align with the compliance controls outlined in the custom standard, ensuring that the policy will enforce or check for the necessary requirements as defined by the standard.

Finally, the last step is to formally associate or map the edited policy with the custom compliance standard.

This is typically done by adding the policy to the standard, which may involve selecting the custom compliance standard from a drop-down menu within the policy settings, confirming that this particular policy should be enforced as part of the compliance checks for that standard.

This ordered process ensures that policies are properly aligned with the organization’s compliance goals and can be enforced and reported on accurately within the security platform.

NEW QUESTION 142

Which alerts are fixed by enablement of automated remediation?
* All applicable open alerts regardless of when they were generated, with alert status updated to

“resolved”
* Only the open alerts that were generated before the enablement of remediation, with alert status updated to “resolved”
* All applicable open alerts regardless of when they were generated, with alert status updated to

“dismissed”
* Only the open alerts that were generated after the enablement of remediation, with alert status updated to

“resolved”
When automated remediation is enabled in Prisma Cloud, it is designed to address all applicable open alerts, regardless of when they were generated. The system automatically applies remediation actions to resolve the identified security issues or compliance violations that triggered the alerts. Once the remediation actions are successfully completed, the system updates the status of the affected alerts to “resolved,” indicating that the security issues have been addressed. This feature helps streamline the remediation process, reducing the manual effort required by security teams and ensuring that security issues are promptly resolved to maintain the integrity and security of the cloud environment.

NEW QUESTION 143

How is the scope of each rule determined in the Prisma Cloud Compute host runtime policy?
* By the collection assigned to that rule
* By the target workload
* By the order in which it is created
* By the type of network traffic it controls
In Prisma Cloud Compute, the scope of each rule within the host runtime policy is determined by the collection assigned to that rule. Collections in Prisma Cloud are logical groupings of resources, such as hosts, containers, or cloud accounts, that share common attributes or security requirements. By associating a rule with a specific collection, administrators can precisely define the context and applicability of the rule, ensuring that the runtime protection mechanisms are accurately targeted and effective. This approach enables granular control over security policies, allowing for tailored security measures that reflect the unique characteristics and needs of different resource groups within the multicloud environment.

NEW QUESTION 144

An administrator has been tasked with a requirement by your DevSecOps team to write a script to continuously query programmatically the existing users, and the user’s associated permission levels, in a Prisma Cloud Enterprise tenant.

Which public documentation location should be reviewed to help determine the required attributes to carry out this step?
* Prisma Cloud Administrator’s Guide (Compute)
* Prisma Cloud API Reference
* Prisma Cloud Compute API Reference
* Prisma Cloud Enterprise Administrator’s Guide

For scripting and programmatically querying user information and permissions within Prisma Cloud, the Prisma Cloud Compute API Reference is the most suitable resource. This API reference provides detailed information on the available endpoints, request formats, and response structures, specifically tailored for compute-related queries, including user and permission management within the Prisma Cloud Compute module. This resource is part of Prisma Cloud’s comprehensive documentation that supports automation and integration with third-party systems, aligning with the platform’s API-first approach to security management.

NEW QUESTION 145

Which policy type in Prisma Cloud can protect against malware?
* Data
* Config
* Network
* Event

Reference:

The Data policy type in Prisma Cloud is designed to protect against malware by scanning data and files for malicious content. This policy type helps in identifying and mitigating malware threats in the cloud environment.

NEW QUESTION 146

A customer is reviewing Container audits, and an audit has identified a cryptominer attack. Which three options could have generated this audit? (Choose three.)
* The value of the mined currency exceeds $100.
* High CPU usage over time for the container is detected.
* Common cryptominer process name was found.
* The mined currency is associated with a user token.
* Common cryptominer port usage was found.

NEW QUESTION 147

What is the function of the external ID when onboarding a new Amazon Web Services (AWS) account in Prisma Cloud?
* It is a UUID that establishes a trust relationship between the Prisma Cloud account and the AWS account in order to extract data.
* It is the default name of the PrismaCloudApp stack.
* It is the resource name for the Prisma Cloud Role.
* It is a unique identifier needed only when Monitor & Protect mode is selected.

NEW QUESTION 148

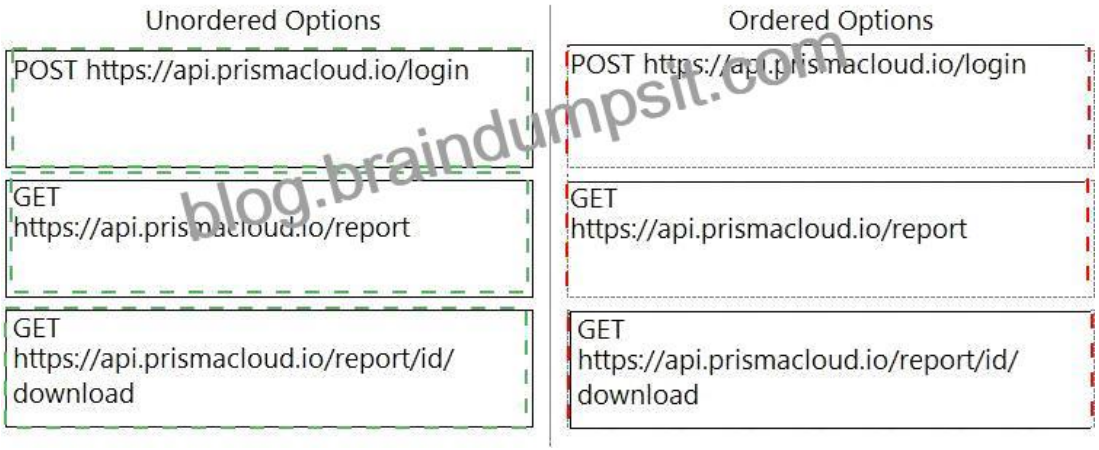
An administrator has been tasked with creating a custom service that will download any existing compliance report from a Prisma Cloud Enterprise tenant.

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

Answer Area



Explanation:

1. Post /Login 2. Get /report 3. Get report/id/download

NEW QUESTION 149

What will happen when a Prisma Cloud Administrator has configured agentless scanning in an environment that also has Host and Container Defenders deployed?

* Agentless scan will automatically be disabled, so Defender scans are the only scans occurring.
* Agentless scans do not conflict with Defender scans, so both will run.
* Defender scans will automatically be disabled, so agentless scans are the only scans occurring.
* Both agentless and Defender scans will be disabled and an error message will be received.

In a Prisma Cloud environment where both agentless scanning and Defender-based scans (Host and Container Defenders) are

configured, there is no inherent conflict between these two scanning methods. Both agentless scans and Defender scans are designed to complement each other, providing comprehensive coverage and depth in the security analysis of the environment. Agentless scans offer a broad, less intrusive overview, while Defender scans provide deep, detailed insights into the security posture. Therefore, both types of scans will run concurrently, enhancing the overall security visibility and protection of the environment without disabling or interfering with each other’s operations.

The agentless scanning architecture lets you inspect a host and the container images in that host without having to install an agent or affecting its execution.

https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/agentless-scanning/onboar

NEW QUESTION 150

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?
* 8084
* 443
* 8083
* 8081

When the administrator wants twistcli to communicate with the Console over HTTPS in a Kubernetes cluster, and considering the load balancer is configured in TCP passthrough mode, A. 8084 is typically the port used for secure HTTPS communication with the Prisma Compute Console. This port will allow twistcli to access the Prisma Compute APIs securely.

https://docs.prismacloudcompute.com/docs/compute_edition_21_04/tools/twistcli.html#connectivity-to-console

NEW QUESTION 151

The compliance team needs to associate Prisma Cloud policies with compliance frameworks. Which option should the team select to perform this task?
* Custom Compliance
* Policies
* Compliance
* Alert Rules

Reference:

compliance/compliance-dashboard.html

NEW QUESTION 152

The development team is building pods to host a web front end, and they want to protect these pods with an application firewall.

Which type of policy should be created to protect this pod from Layer7 attacks?
* The development team should create a WAAS rule for the host where these pods will be running.
* The development team should create a WAAS rule targeted at all resources on the host.
* The development team should create a runtime policy with networking protections.
* The development team should create a WAAS rule targeted at the image name of the pods.

To protect the pods hosting a web front end from Layer 7 attacks, the development team should create a Web Application and API

Security (WAAS) rule targeted at the image name of the pods. This approach allows the policy to specifically protect the applications running within the pods against sophisticated attacks that target the application layer.

https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/waas/deploy_waas