KaozhengPro

IT認證考試題庫

專業平臺

考證寶提供最新考古題與模擬試題
協助您高效通過認證考試

www.kaozhengpro.com

Exam : **CloudSec-Pro**

Title : Palo Alto Networks Cloud Security Professional

Version : DEMO

1.What improves product operationalization by adding visibility into feature utilization and missed opportunities?
A. Adoption Advisor
B. Alarm Advisor
C. Alert Center
D. Alarm Center
Answer: A
Explanation:
The Adoption Advisor is a feature within Prisma Cloud that aims to improve product operationalization. It provides visibility into how features are utilized, identifies unused capabilities, and suggests ways to leverage the full potential of the platform.
Therefore, Option A: Adoption Advisor is the correct answer.

2.The security team wants to enable the “block” option under compliance checks on the host.
What effect will this option have if it violates the compliance check?
A. The host will be taken offline.
B. Additional hosts will be prevented form starting.
C. Containers on a host will be stopped.
D. No containers will be allowed to start on that host.
Answer: D
Explanation:
Enabling the "block" option under compliance checks on a host in Prisma Cloud signifies a strict enforcement policy, where any container that violates specified compliance checks will be prevented from starting on that host. This preventive measure is crucial for maintaining a secure and compliant cloud environment, ensuring that only containers that meet the organization's compliance and security standards are allowed to run. This approach aligns with Prisma Cloud's proactive security posture management, where potential risks are mitigated before they can impact the cloud environment.
https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/compliance/manage_compliance

3.In Azure, what permissions need to be added to Management Groups to allow Prisma Cloud to calculate net effective permissions?
A. Microsoft.Management/managementGroups/descendants/read
B. Microsoft.Management/managementGroups/descendants/calculate
C. PaloAltoNetworks.PrismaCloud/managementGroups/descendants/read
D. PaloAltoNetworks.PrismaCloud/managementGroups/
Answer: A
Explanation:
In Azure, to enable Prisma Cloud to calculate net effective permissions across Management Groups, the necessary permission is "Microsoft.Management/managementGroups/descendants/read." This permission grants Prisma Cloud the ability to read the management group hierarchy and the related details, allowing for a comprehensive analysis of the effective permissions applied across different levels of the management group structure. By having this level of access, Prisma Cloud can accurately assess and report on the permissions assigned to various resources and identities within the Azure environment,

facilitating better security and compliance management.

4.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
Explanation:
CloudFormation templates, used to describe and provision all the infrastructure resources in cloud environments, support various elements including resources, mappings, parameters, and outputs. However, scan support for CloudFormation templates does not currently exist for nested references, macros, or intrinsic functions (option A). These advanced CloudFormation features can introduce complexity in scanning and interpreting the templates accurately for security and compliance checks.
Reference: https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/prisma-cloud-devops-security/use-the-prisma-cloud-iac-scan-rest-api.html

5.The Unusual protocol activity (Internal) network anomaly is generating too many alerts. An administrator has been asked to tune it to the option that will generate the least number of events without disabling it entirely.
Which strategy should the administrator use to achieve this goal?
A. Disable the policy
B. Set the Alert Disposition to Conservative
C. Change the Training Threshold to Low
D. Set Alert Disposition to Aggressive
Answer: B
Explanation:
To reduce the number of alerts generated by the "Unusual protocol activity (Internal)" network anomaly without entirely disabling the policy, setting the Alert Disposition to Conservative (option B) is the most effective strategy. This configuration adjusts the sensitivity of the anomaly detection, reducing the likelihood of false positives and minimizing alert fatigue without compromising the ability to detect genuine security threats. By adopting a more conservative approach to anomaly detection, the administrator can ensure that only the most significant and potentially harmful activities trigger alerts, thus maintaining a balance between security vigilance and operational efficiency.