Atmic Networks

CERTIFICATION EXAM SUPPORT

EXAM PREPARATION MATERIAL

Practice files designed to help you understand exam patterns, question styles and the overall assessment format.

IMPORTANT NOTE

> **Please note that these files may not be up to date. However, the questions will help you understand the exam format and typical question patterns.**

Stay connected with our support team
for the latest file updates and exam-related information.

www.atmicnetworks.com

Knowledge that moves beyond memorization.

www.atmicnetworks.com

Question: 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.

Question: 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.

Question: 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.

https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA14u000000oMkpCAE&lang=en_US%E2%80%A9&refURL=http%3A%2F%2Fknowledgebase.paloaltonetworks.com%2FKCSArticleDetail

Question: 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: A,D,E

Explanation:

Palo Alto Networks' Enterprise DLP service and provides data classification that includes built-in data profiles with data patterns that match sensitive information such as PII, health care, financial information and Intellectual Property. In addition to protecting your confidential and sensitive data, your data is also protected against threats—known and unknown (zero-day) malware—using the Palo Alto Networks' WildFire service.

Question: 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: D

Explanation:

https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/runtime_defense/runtime_defense_containers

www.atmicnetworks.com

Question: 6

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 certificate.2.Retrieve the Prisma Cloud Console images using 'docker pull'.

D. To retrieve Prisma Cloud Console images using URL auth:1.Access registry-auth.twistlock.com, and authenticate using the user certificate.2.Retrieve the Prisma Cloud Console images using 'docker pull'.

Answer: B

Explanation:

Retrieving Prisma Cloud Console images involves accessing a specific registry provided by Palo Alto Networks and authenticating using basic authentication with 'docker login'. Once authenticated, the user can pull the Prisma Cloud Console images using the 'docker pull' command. This process is part of the initial setup for deploying Prisma Cloud Console in an environment, allowing users to obtain the necessary images to run the Console, which serves as the central management interface for Prisma Cloud. The detailed steps, including the specific registry URL and authentication method, are typically provided in the Prisma Cloud documentation, ensuring that users have the information needed to successfully retrieve and deploy Console images.

Question: 7

Which two statements are true about the differences between build and run config policies? (Choose two.)

A. Run and Network policies belong to the configuration policy set.

B. Build and Audit Events policies belong to the configuration policy set.

C. Run policies monitor resources, and check for potential issues after these cloud resources are deployed.

D. Build policies enable you to check for security misconfigurations in the IaC templates and ensure that these issues do not get into production.

E. Run policies monitor network activities in your environment, and check for potential issues during runtime.

Answer: C,D

Explanation:

In the context of Prisma Cloud, Build and Run policies serve distinct purposes in securing cloud environments. Build policies are designed to evaluate Infrastructure as Code (IaC) templates before deployment. These policies help identify and remediate security misconfigurations in the development phase, ensuring that vulnerabilities are addressed before the infrastructure is provisioned. This proactive approach enhances security by preventing misconfigurations from reaching production environments.

On the other hand, Run policies are applied to resources that are already deployed in the cloud. These policies continuously monitor the cloud environment, detecting and alerting on potential security issues that arise in the runtime. Run policies help maintain the security posture of cloud resources by identifying deviations from established security baselines and enabling quick remediation of identified issues.

Both Build and Run policies are integral to a comprehensive cloud security strategy, addressing security concerns at different stages of the cloud resource lifecycle—from development and deployment to ongoing operation.

Question: 8

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: D

Explanation:

In Prisma Cloud, when anomalies are detected and the security team chooses to Relearn on a specific image, the existing behavioral model for that image is not deleted. Instead, the system retains the model and enters a new learning period, during which it observes the behavior of the container based on the image. If new behaviors are observed during this period, they are added to the existing model, thereby refining and updating the model to reflect the current operational profile of the container. This approach allows for dynamic adaptation to changes in container behavior while preserving the valuable insights and patterns already established in the model. The Relearn function is part of Prisma Cloud's adaptive capabilities, enabling it to maintain accurate and up-to-date behavioral models that reflect the evolving nature of containerized applications.

Question: 9

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

Explanation:

B --> Anomaly Trusted List—Exclude trusted IP addresses when conducting tests for PCI compliance or penetration testing on your network. Any addresses included in this list do not generate alerts against the Prisma Cloud Anomaly Policies that detect unusual network activity such as the policies that detect internal port scan and port sweep activity, which are enabled by default. C --> Trusted Alert IP Addresses—If you have internal networks that connect to your public cloud infrastructure, you can add these IP address ranges (or CIDR blocks) as trusted ... Prisma Cloud default network policies that look for internet exposed instances also

do not generate alerts when the source IP address is included in the trusted IP address list and the account hijacking anomaly policy filters out activities from known IP addresses. Also, when you use RQL to query network traffic, you can filter out traffic from known networks that are included in the trusted IP address list.

For a customer who does not want alerts to be generated from network traffic originating from trusted internal networks, the appropriate setting is C. Trusted Alert IP Addresses. This setting allows for specifying certain IP addresses as trusted, meaning alerts will not be triggered by activities from these IPs, ensuring that internal network traffic is not flagged as potentially malicious.

Question: 10

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: C

Explanation:

To investigate the runtime aspects of a potential data exfiltration attempt, the SecOps lead in Prisma Cloud Compute should focus on areas that provide insights into runtime activity and potential threats. C. The SecOps lead should use the Incident Explorer page and Monitor > Events > Container Audits. These sections provide detailed information on security incidents and container-level activities, enabling a thorough investigation into the runtime behavior that might indicate a security issue.

Question: 11

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: B,C

Explanation:

RESOURCE_DELETED Resource was deleted. USER_DISMISSED Alert was dismissed or snoozed by the Prisma Cloud administrator with role of System admin, Account Group Admin, or Account and Cloud Provisioning Admin. POLICY_UPDATED Policy was updated. This status indicates a change in the policy RQL that results in a resource not being in scope for the policy evaluation.

https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA14u0000004OQ2CAM

Question: 12

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: B,D,E

Explanation:

Onboarding an account for Data Security involves several critical steps to ensure comprehensive coverage and effective monitoring. The steps involved include B. Create a Cloudtrail with SNS Topic to track and manage API calls and relevant notifications, D. Enter the RoleARN and SNSARN to provide necessary access and integration points for data security functions, and E. Create a S3 bucket which serves as a storage solution for logging and data capture essential for security analysis.

Question: 13

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: C

Explanation:

By default Prisma Cloud listens on: 8083 HTTPS management port for access to Console. 8084 WSS port for Defender to Console communication.

https://docs.paloaltonetworks.com/prisma/prisma-cloud/19-11/prisma-cloud-compute-edition-admin/install/install_kubernetes

Question: 14

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: B,C,E

Explanation:

In the case of identifying a cryptominer attack through container audits, the options that could have generated this audit include B. High CPU usage over time for the container is detected, which is a common indicator of cryptomining activity as it consumes significant computational resources, C. Common cryptominer process name was found, which directly indicates the presence of cryptomining based on known malicious processes, and E. Common cryptominer port usage was found, suggesting cryptomining activity based on network behavior typical of such attacks.

Question: 15

Which step is included when configuring Kubernetes to use Prisma Cloud Compute as an admission controller?

A. copy the Console address and set the config map for the default namespace.

B. create a new namespace in Kubernetes called admission-controller.

C. enable Kubernetes auditing from the Defend > Access > Kubernetes page in the Console.

D. copy the admission controller configuration from the Console and apply it to Kubernetes.

Answer: D

Explanation:

When configuring Kubernetes to use Prisma Cloud Compute as an admission controller, a crucial step involves D. copy the admission controller configuration from the Console and apply it to Kubernetes. This step is essential for integrating Prisma Cloud Compute's security controls directly into the Kubernetes admission process, enabling real-time security assessments and policy enforcement for new or modified resources within the cluster.

https://docs.paloaltonetworks.com/prisma/prisma-cloud/20-04/prisma-cloud-compute-edition-admin/access_control/open_policy_agent.html step 2

Question: 16

A Prisma Cloud administrator is onboarding a single GCP project to Prisma Cloud. Which two steps can be performed by the Terraform script? (Choose two.)

A. enable flow logs for Prisma Cloud.

B. create the Prisma Cloud role.

C. enable the required APIs for Prisma Cloud.

D. publish the flow log to a storage bucket.

Answer: B,C

Explanation:

When a Prisma Cloud administrator is onboarding a single GCP project to Prisma Cloud, the Terraform script can perform several steps to facilitate this integration. The steps include B. create the Prisma Cloud role, which is essential for defining the permissions and capabilities that Prisma Cloud will have within the GCP environment, and C. enable the required APIs for Prisma Cloud, ensuring that Prisma Cloud can access the necessary GCP services and features for comprehensive cloud security management.

Question: 17

Which statement about build and run policies is true?

A. Build policies enable you to check for security misconfigurations in the IaC templates.

B. Every type of policy has auto-remediation enabled by default.

C. The four main types of policies are: Audit Events, Build, Network, and Run.

D. Run policies monitor network activities in the environment and check for potential issues during runtime.

Answer: A

Explanation:

A true statement about build and run policies is A. Build policies enable you to check for security misconfigurations in the IaC templates. This capability is crucial for identifying potential security issues early in the development process, allowing for proactive mitigation before deployment, thereby enhancing the overall security posture of the applications and infrastructure being developed.

Question: 18

An administrator sees that a runtime audit has been generated for a host. The audit message is:

"Service postfix attempted to obtain capability SHELL by executing /bin/sh /usr/libexec/postfix/postfix- script.stop. Low severity audit, event is automatically added to the runtime model"

Which runtime host policy rule is the root cause for this runtime audit?

A. Custom rule with specific configuration for file integrity

B. Custom rule with specific configuration for networking

C. Default rule that alerts on capabilities

D. Default rule that alerts on suspicious runtime behavior

Answer: D

Explanation:

For a runtime audit generated for a host with a message indicating a service attempting to obtain capability by

executing a script, the root cause for this runtime audit is most likely related to D. Default rule that alerts on suspicious runtime behavior. This default rule is designed to flag unusual or potentially harmful activities that could indicate a security risk, prompting further investigation.

Question: 19

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

Explanation:

The Prisma Cloud Compute Edition is identified as B. Downloadable, self-hosted software. This option indicates that Prisma Cloud Compute Edition is a solution that organizations can deploy within their own infrastructure, providing them with control over the installation, configuration, and management of the security platform.

Reference: https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/welcome/ pcee_vs_pcce.html

Question: 20

Which type of compliance check is available for rules under Defend > Compliance > Containers and Images > CI?

A. Host

B. Container

C. Functions

D. Image

Answer: D

Explanation:

In the context of Defend > Compliance > Containers and Images > CI within Prisma Cloud by Palo Alto Networks, the compliance checks are focused on the security posture and compliance of container images. Therefore, the type of compliance check available under this section would be related to Images, ensuring they adhere to security best practices and compliance standards before being deployed.

Question: 21

The security team wants to protect a web application container from an SQLi attack. Which type of policy should the administrator create to protect the container?

A. CNAF

B. Runtime

C. Compliance

D. CNNF

Answer: A

Explanation:

To protect a web application container from an SQL Injection (SQLi) attack, the administrator should create a

Cloud Native Application Firewall (CNAF) policy. CNAF policies are designed to protect applications running in containers from various types of attacks, including SQLi, by inspecting the traffic going to and from the containerized applications and blocking malicious requests.

Reference: https://docs.paloaltonetworks.com/prisma/prisma-cloud/20-09/prisma-cloud-compute-edition-admin/firewalls/waas

Question: 22

An S3 bucket within AWS has generated an alert by violating the Prisma Cloud Default policy “AWS S3 buckets are accessible to public”. The policy definition follows:

config where cloud.type = 'aws' AND api.name='aws-s3api-get-bucket-acl' AND
json.rule="((((acl.grants[? (@.grantee=='AllUsers')] size > 0) or policyStatus.isPublic is true) and publicAccessBlockConfiguration does not exist) or ((acl.grants[?(@.grantee=='AllUsers')] size > 0) and publicAccessBlockConfiguration.ignorePublicAcis is false) or (policyStatus.isPublic is true and publicAccessBlockConfiguration.restrictPublicBuckets is false)) and websiteConfiguration does not exist"

Why did this alert get generated?

A. an event within the cloud account

B. network traffic to the S3 bucket

C. configuration of the S3 bucket

D. anomalous behaviors

Answer: C

Explanation:

The alert "AWS S3 buckets are accessible to public" is generated due to the configuration of the S3 bucket, which has been set in a way that allows public access. The policy definition provided checks for various conditions that would make an S3 bucket publicly accessible, such as grants to 'AllUsers', the absence of a 'publicAccessBlockConfiguration', or specific configurations that do not restrict public access. Therefore, the alert is triggered by the configuration settings of the S3 bucket that violate the policy's

criteria for public accessibility.

Question: 23

DRAG DROP

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	Ordered Options
Add the custom compliance standard from the drop-down menu	
Create the custom compliance standard	
Edit the Policy	
Click on Compliance Standards	

Answer:

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_c

hecks.html#creating-a-new-custom-check

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.

Question: 24

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: C

Explanation:

Block — Defender stops the entire container if a process that violates your policy attempts to run.

https://docs.prismacloudcompute.com/docs/enterprise_edition/runtime_defense/runtime_defense_containers.html#_effect

Question: 25

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 cluster. A onebox deployment should be used.

B. Download and extract the release tarballEnsure that each node has its own storage for Console data Create the Console task definitionDeploy the task definition

C. Download and extract release tarball Download task from AWSCreate the Console task definition Deploy the task definition

D. Download and extract the release tarball Create an EFS file system and mount to each node in the cluster Create the Console task definition Deploy the task definition

Answer: D

Explanation:

Reference: https://docs.paloaltonetworks.com/prisma/prisma-cloud/19-11/prisma-cloud-compute-edition-admin/install/install_amazon_ecs.html

To install the Console in an Amazon ECS Cluster, the steps involve downloading and extracting the release tarball, which contains the necessary files for the Console. Then, an Amazon Elastic File System (EFS) should be created and mounted to each node in the ECS cluster to provide shared storage for Console data. Following this, a Console task definition needs to be created in ECS, which defines how the Console container should run. Finally, this task definition is deployed to the ECS cluster to start the Console.

www.atmicnetworks.com

Question: 26

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 ConsoleUpgrade Supervisor Consoles

D. Upgrade Central Console Upgrade all Supervisor Consoles

Answer: A

Explanation:

When you have one or more tenant or scale Projects, upgrade all Supervisors before upgrading the Central Console. https://docs.paloaltonetworks.com/prisma/prisma-cloud/20-09/prisma-cloud- compute-edition-admin/upgrade/upgrade_process

Question: 27

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: A,C

Explanation:

https://docs.paloaltonetworks.com/prisma/prisma-cloud/20-09/prisma-cloud-compute-edition-admin/upgrade/upgrade_process

Question: 28

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

Explanation:

In the context of setting anomaly alert intensities in Prisma Cloud, an intensity setting of "Medium" could be used for the measurement of 100 events over 30 days. This setting indicates a moderate level of anomaly detection sensitivity, which is suitable for environments where there is a need to balance between detecting potential security issues and minimizing false positives.

Reference: https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/manage- prisma-cloud- administrators/define-prisma-cloud-enterprise-settings.html

https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/manage-prisma- cloud-administrators/define-prisma-cloud-enterprise-settings

Question: 29

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: D

Explanation:

https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/tools/twistcli_scan_images

Question: 30

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: C

Explanation:

To protect pods in an environment from Cross-Site Scripting (XSS) attacks, the development team should create a Container Cloud Native Application Firewall (CNAF) policy. This policy should be targeted at the specific resource (e.g., a particular pod or set of pods), with the option for XSS protection checked, and the action set to "prevent." This configuration ensures that any XSS attacks directed at the targeted containers are effectively blocked.

Question: 31

The Prisma Cloud administrator has configured a new policy.

Which steps should be used to assign this policy to a compliance standard?

A. Edit the policy, go to step 3 (Compliance Standards), click + at the bottom, select the compliance standard, fill in the other boxes, and then click Confirm.

B. Create the Compliance Standard from Compliance tab, and then select Add to Policy.

C. Open the Compliance Standards section of the policy, and then save.

D. Custom policies cannot be added to existing standards.

Answer: A

Explanation:

To assign a new policy to a compliance standard in Prisma Cloud, the administrator needs to edit the policy and navigate to the step where compliance standards are managed. By clicking the '+' button, the administrator can add the policy to a specific compliance standard, provide necessary details, and confirm the assignment. This integrates the custom policy into the chosen compliance standard, ensuring that compliance checks include the newly defined policy criteria.

Question: 32

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

Explanation:

The correct command to generate the YAML file for Defender install in a Kubernetes cluster, considering the console and websocket addresses, as well as the admin user, would typically involve specifying the addresses and user details. The option D seems most aligned with standard practices for such commands, where you export the Defender configuration for Kubernetes, specifying the console and websocket addresses along with the user details.

Reference: https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/install/ install_kubernetes.html

Question: 33

Which options show the steps required after upgrade of Console?

A. Uninstall Defenders Upgrade Jenkins PluginUpgrade 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

Explanation:

After the Console has been upgraded, check and upgrade any of the Defenders that have reached the end of their support lifecycle (Defenders are backward compatible for N-2 releases). The Defender release image is built from the UBI8-minimal base image and on upgrade it is a full container image upgrade, which means that the old Defender container is replaced with a new container. Then, upgrade all other Prisma Cloud components, such as the Jenkins plugin. https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin- compute/upgrade/upgrade_process_saas

Question: 34

An organization wants to be notified immediately to any “High Severity” alerts for the account group “Clinical Trials” via Slack.

Which option shows the steps the organization can use to achieve this goal?

A. 1. Configure Slack Integration2.Create an alert rule and select “Clinical Trials” as the account group3.Under the “Select Policies” tab, filter on severity and select “High”4.Under the Set Alert Notification tab, choose Slack and populate the channel5.Set Frequency to “As it Happens”

B. 1. Create an alert rule and select “Clinical Trials” as the account group2.Under the “Select Policies”

tab, filter on severity and select “High”3.Under the Set Alert Notification tab, choose Slack and populate the channel4.Set Frequency to “As it Happens”5.Set up the Slack Integration to complete the configuration

C. 1. Configure Slack Integration2.Create an alert rule3.Under the “Select Policies” tab, filter on severity and select “High”4.Under the Set Alert Notification tab, choose Slack and populate the channel5.Set Frequency to “As it Happens”

D. 1. Under the “Select Policies” tab, filter on severity and select “High”2.Under the Set Alert Notification tab, choose Slack and populate the channel3.Set Frequency to “As it Happens”4.Configure Slack Integration5.Create an Alert rule

Answer: A

Explanation:

To achieve immediate notification for "High Severity" alerts for a specific account group via Slack, the steps outlined in option A provide a comprehensive and effective approach. Firstly, configuring the Slack Integration establishes the necessary communication channel between Prisma Cloud and the Slack workspace. Creating an alert rule with the specified account group and severity filters ensures that only relevant alerts trigger notifications. Selecting Slack as the notification channel and setting the frequency to "As it Happens" ensures real-time alerting for critical issues. This method leverages Prisma Cloud's alerting capabilities and Slack's real-time messaging platform to promptly notify the security team, enabling swift action to mitigate risks. This approach is in line with Prisma Cloud's flexible and configurable alerting system, designed to integrate with various external platforms for efficient incident response.

Question: 35

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: C

Explanation:

To add AWS accounts to the Prisma Cloud Enterprise tenant, the correct API endpoint is option C: https://api.prismacloud.io/cloud/aws. This endpoint is specifically designed for integrating cloud accounts with Prisma Cloud, enabling centralized visibility and security posture management across multiple cloud environments. By using this API endpoint, each AWS account can be individually onboarded to the Prisma Cloud platform, allowing for immediate posture visibility and consistent security policy enforcement across the newly acquired company's extensive AWS footprint. This process aligns with Prisma Cloud's capabilities for multi-cloud security and compliance management, ensuring that the onboarding of cloud accounts is both efficient and aligned with the platform's best practices for cloud security.

Question: 36

A security team has a requirement to ensure the environment is scanned for vulnerabilities. What are three options for configuring vulnerability policies? (Choose three.)

A. individual actions based on package type

B. output verbosity for blocked requests

C. apply policy only when vendor fix is available

D. individual grace periods for each severity level

E. customize message on blocked requests

Answer: A,C,D

Explanation:

https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/vulnerability_management/vuln_management_rules

Configuring vulnerability policies within Prisma Cloud involves several options that cater to different aspects of vulnerability management and policy enforcement. Options A, C, and D are valid configurations for vulnerability policies:

A . Individual actions based on package type allow for tailored responses to vulnerabilities found in specific types of software packages, enabling more granular control over the remediation process.

C . Applying policies only when a vendor fix is available helps prioritize the remediation of vulnerabilities for which a patch or update has been released by the software vendor, ensuring efficient use of resources in addressing the most actionable security issues.

D . Setting individual grace periods for each severity level allows organizations to define different time frames for addressing vulnerabilities based on their severity, enabling a prioritized and risk based approach to vulnerability management.

These configurations support a comprehensive vulnerability management strategy by allowing customization and prioritization based on the nature of the vulnerability, the availability of fixes, and the risk level associated with each vulnerability.

Question: 37

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.

Question: 38

What is the behavior of Defenders when the Console is unreachable during upgrades?

A. Defenders continue to alert, but not enforce, using the policies and settings most recently cached before upgrading the Console.

B. Defenders will fail closed until the web-socket can be re-established.

C. Defenders will fail open until the web-socket can be re-established.

D. Defenders continue to alert and enforce using the policies and settings most recently cached before upgrading the Console.

Answer: D

Explanation:

When the Console is unreachable during upgrades, Defenders continue to alert and enforce using the policies and settings most recently cached before the upgrade (option D). This behavior ensures that security enforcement remains active and consistent, even when the central management console is temporarily unavailable. The cached policies enable Defenders to maintain the security posture based on the last known configuration, ensuring continuous protection against threats and compliance with established security policies. This approach reflects Prisma Cloud's design principle of ensuring uninterrupted security enforcement, thereby safeguarding the environment against

potential vulnerabilities during maintenance periods.

Reference: https://docs.paloaltonetworks.com/prisma/prisma-cloud/20-09/prisma-cloud-compute- edition-admin/upgrade/upgrade_process.html

Question: 39

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

Explanation:

The activities listed (Backdoor account access, Hijacked processes, Lateral movement, Port scanning) are categorized as incidents (option B). Incidents represent security events or patterns of activity that indicate potential security breaches or malicious behavior within the environment. Prisma Cloud identifies and classifies such activities as incidents to highlight significant security concerns that require investigation and potential remediation. This categorization helps security teams prioritize their response efforts, focusing on activities that pose a real threat to the integrity and security of the cloud environment. By distinguishing incidents from other types of security findings, Prisma Cloud enables more effective incident response and threat management processes.

Question: 40

DRAG DROP

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

Unordered Options	Ordered Options
POST https://api.prismacloud.io/login	
GET https://api.prismacloud.io/access_keys	
PATCH https://api.prismacloud.io/access_keys/<id>/status/<status>	

Answer:

Explanation:

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

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

PATCH https://api.prismacloud.io/access_keys/<id>/status/<status>

To write a script that automatically deactivates access keys that have not been used for 30 days, an administrator would need to follow an ordered sequence of API calls to the Prisma Cloud platform.

The first API call must authenticate the script with the Prisma Cloud API, which is typically done using a POST request to the login endpoint. This step is necessary to establish a session and retrieve an authentication token required for subsequent API calls.

Once the script is authenticated, the next call is a GET request to the access_keys endpoint. This retrieves a list of all

access keys within the environment. The script can then parse through these keys to determine which ones have not been used within the specified timeframe of 30 days.

For each access key that meets the criteria (unused for 30 days), the script must send a PATCH request to the specific access key's endpoint, which includes the access key ID and the desired status. This request will change the status of the access key to 'inactive' or a similar status that denotes deactivation.

Following this ordered sequence ensures that the script systematically authenticates, evaluates, and updates the status of access keys based on their usage, thereby maintaining security and compliance within the Prisma Cloud environment.

Question: 41

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

Explanation:

To authenticate to Prisma Cloud Enterprise programmatically, the use of an access key is the most suitable method among the given options. Access keys, typically consisting of an Access Key ID and Secret Access Key, are used for programmatic calls to the Prisma Cloud API. This method enables secure, authenticated API requests to Prisma Cloud services without requiring manual user intervention, which is essential for automation and integration with CI/CD pipelines.

Reference to the use of access keys for programmatic access can often be found in the API documentation of cloud security platforms like Prisma Cloud. While specific documentation from Prisma Cloud is not directly quoted here, the general practice across cloud services (AWS, Azure, GCP) supports the use of access keys for API authentication, making it a verified approach for Prisma Cloud as well.

Reference: https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/get- started-with- prisma-cloud/access-the-prisma-cloud-api.html

Question: 42

Which option shows the steps to install the Console in a Kubernetes Cluster?

A. Download the Console and Defender image Generate YAML for DefenderDeploy Defender YAML using kubectl

B. Download and extract release tarball Generate YAML for ConsoleDeploy Console YAML using kubectl

C. Download the Console and Defender image Download YAML for Defender from the document site Deploy Defender YAML using kubectl

D. Download and extract release tarball Download the YAML for Console Deploy Console YAML using kubectl

Answer: B

Explanation:

The installation of the Prisma Cloud Console in a Kubernetes cluster involves a series of steps that start with preparing the necessary deployment configurations, typically provided as YAML files. The process begins by downloading and extracting the release tarball, which contains the necessary files and instructions for the deployment. After extracting the tarball, you generate YAML files for the Console deployment. These YAML files define the Kubernetes resources needed to deploy and run the Console, such as Deployments, Services, and ConfigMaps. Finally, you deploy the Console by applying the generated YAML files using the kubectl command, which communicates with the Kubernetes API to create the specified resources in your cluster.

This process is aligned with Kubernetes best practices for deploying applications and is indicative of the steps required for deploying complex applications like the Prisma Cloud Console. The method ensures that all necessary configurations and dependencies are correctly defined and deployed in the Kubernetes environment.

Question: 43

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

Explanation:

Reference: https://blog.paloaltonetworks.com/prisma-cloud/protect-serverless-functions/

Automatically protecting all Lambda functions with runtime protection in Prisma Cloud can be achieved by configuring a serverless auto-protect rule. This feature allows for the automatic application of runtime protection policies to all Lambda functions without the need for manual intervention or embedding defenders in each function. The auto-protect rule ensures that as new Lambda functions are deployed, they are automatically protected based on the predefined security policies, maintaining a consistent security posture across all serverless functions.

This approach leverages the capabilities of Prisma Cloud to integrate seamlessly with serverless architectures, providing a layer of security that is both comprehensive and adaptive to the dynamic nature of serverless computing. By automating the protection process, organizations can ensure that their serverless functions are always covered by the latest security policies, reducing the risk of vulnerabilities and attacks.

Question: 44

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: B

Explanation:

Prisma Cloud supports Single Sign-On (SSO) integration through Security Assertion Markup Language (SAML), enabling users to authenticate using their existing identity providers (IdPs) such as Okta, Azure Active Directory, PingID, among others. This SSO integration allows for a seamless user authentication experience, where users can log in to Prisma Cloud using their credentials managed by their organization's IdP. The SAML protocol facilitates this by allowing secure exchange of authentication and authorization data between the IdP and Prisma Cloud.

This integration enhances security by centralizing user authentication, reducing the number of passwords users need to remember, and enabling organizations to enforce their security policies, such as multi-factor authentication (MFA) and password complexity, across their cloud security tools. SAML support is a common feature in cloud security platforms for integrating with various IdPs, making it a verified approach for Prisma Cloud as well.

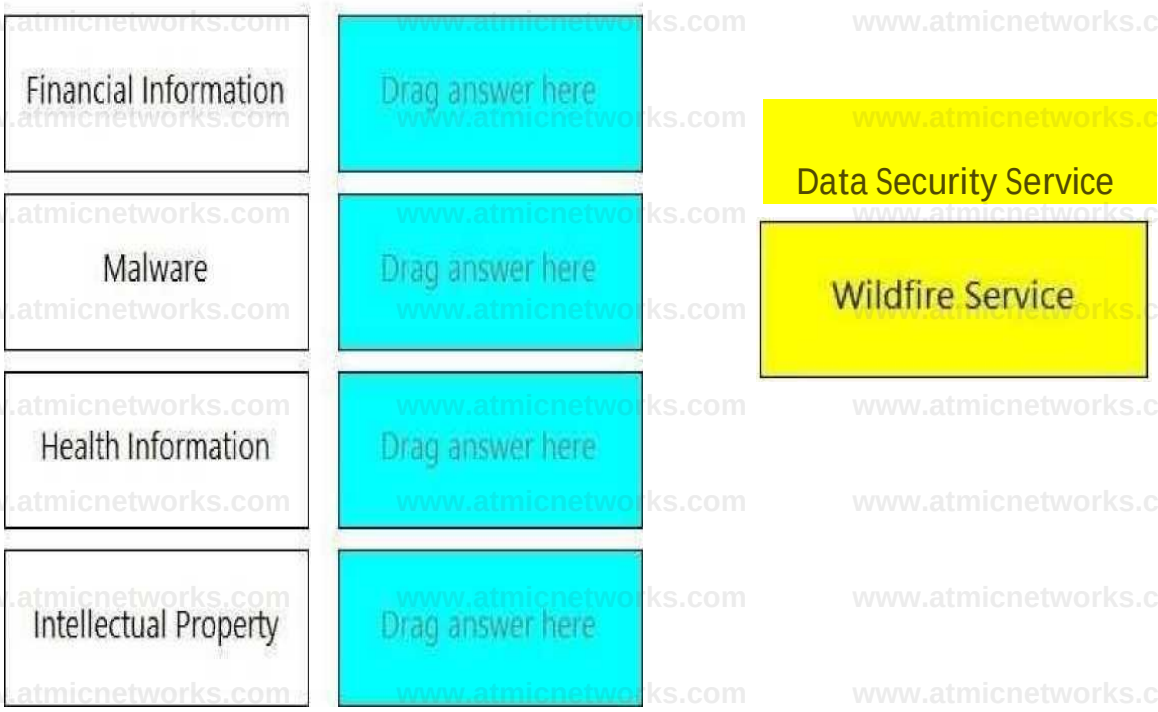
Question: 45

DRAG DROP

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



Explanation:

Answer:

Data Security Service

WildFire Service

Data Security Service

Data Security Service

Reference:

https://www.paloaltonetworks.com/prisma/cloud/cloud-data-security

Question: 46

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: A,C

Explanation:

To scan container images in Jenkins pipelines, two effective methods are using twistcli and the Compute Jenkins plugin. twistcli is a command-line tool provided by Prisma Cloud that allows for the scanning of container images for vulnerabilities and compliance issues directly from the CI/CD pipeline. It can be integrated into Jenkins jobs as a build or post-build step to automatically scan images as part of the build process.

The Compute Jenkins plugin is specifically designed for integration with Jenkins, providing a more seamless and automated way to include Prisma Cloud's security scanning capabilities within Jenkins pipelines. This

plugin enables Jenkins to trigger image scans with Prisma Cloud directly and can fail builds based on scan results, ensuring that only secure and compliant images are pushed through the CI/CD pipeline.

Both twistcli and the Compute Jenkins plugin are designed to integrate Prisma Cloud's security capabilities into the CI/CD process, enabling DevOps teams to identify and fix security issues early in the development lifecycle.

Question: 47

A customer wants to harden its environment from misconfiguration.

Prisma Cloud Compute Compliance enforcement for hosts covers which three options? (Choose three.)

A. Docker daemon configuration files

B. Docker daemon configuration

C. Host cloud provider tags

D. Host configuration

E. Hosts without Defender agents

Answer: A,B,D

Explanation:

Prisma Cloud Compute Compliance enforcement for hosts covers several aspects to ensure a secure and compliant host environment, particularly within containerized environments. These include:

Docker daemon configuration files: Ensuring that Docker daemon configuration files are set up according to best security practices is crucial. These files contain various settings that control the behavior of the Docker daemon, and misconfigurations can lead to security vulnerabilities.

Docker daemon configuration: Beyond just the configuration files, the overall configuration of the Docker daemon itself is critical. This encompasses runtime settings and command-line options that determine how Docker containers are executed and managed on the host.

Host configuration: The security of the underlying host on which Docker and other container runtimes are installed is paramount. This includes the configuration of the host's operating system, network settings, file permissions, and other system-level settings that can impact the security of the containerized applications running on top.

By focusing on these areas, Prisma Cloud ensures that not just the containers but also the environment they run in is secure, adhering to compliance standards and best practices to mitigate risks associated with containerized deployments.

Question: 48

A Prisma Cloud administrator is tasked with pulling a report via API. The Prisma Cloud tenant is located on app2.prismacloud.io.

What is the correct API endpoint?

A. https://api.prismacloud.io

B. https://api2.eu.prismacloud.io

C. httsp://api.prismacloud.cn

D. https://api2.prismacloud.io

Answer: D

Explanation:

https://prisma.pan.dev/api/cloud/api-urls/

When accessing the Prisma Cloud API for a tenant located on app2.prismacloud.io, the correct API endpoint to use would be https://api2.prismacloud.io. This endpoint corresponds to the Prisma Cloud service instance hosted on app2.prismacloud.io, ensuring that API requests are directed to the correct instance of the service for processing.

The use of api2 in the URL indicates that this is the second instance or a different geographical or functional partition of the Prisma Cloud service, which might be used for load balancing, redundancy, or serving different sets of users. It is crucial to use the correct endpoint corresponding to the Prisma Cloud console URL to ensure successful API communication and authentication.

Question: 49

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

Explanation:

To view the vulnerabilities identified on a host, navigating to the "Monitor > Vulnerabilities > Hosts" section within the Prisma Cloud Console is the correct approach. This section is specifically designed to provide a comprehensive overview of all detected vulnerabilities within the host environment, offering detailed insights into each vulnerability's nature, severity, and potential impact.

This pathway allows users to efficiently assess the security posture of their hosts, prioritize vulnerabilities based on their severity, and take appropriate remediation actions. The "Hosts" section under "Vulnerabilities" is tailored to display vulnerabilities related to host configurations, installed software, and other host-level security concerns, making it the ideal location within the Prisma Cloud Console for this purpose.

Question: 50

DRAG DROP

Order the steps involved in onboarding an AWS Account for use with Data Security feature.

Answer Area

Unordered Options	Ordered Options
Enter RoleARN and SNSARN	
Create Stack	
Enter SNS Topic in CloudTrail	
Create CloudTrail with S3 as storage	

Answer:

Explanation:

1 -Create Stack
2 - Ener SNS Topic in Cloudtrail
3 - Create Cloudtrail with S3 as Storage
4 - Enter RoleARN and SNSARN

https://docs.prismacloud.io/en/classic/cspm-admin-guide/prisma-cloud-data-security/enable-data- security-module/enable-data-security-for-aws-org-account

Question: 51

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: B,C,E

Explanation:

To configure serverless scanning in a cloud security platform like Prisma Cloud, the system needs to know where (Region) the serverless functions are deployed, how to access them (Credential), and on which cloud platform they are running (Provider). These settings ensure that the scanning tool can accurately locate and authenticate to the serverless functions across different cloud environments for vulnerability assessment. This aligns with the principle of providing comprehensive visibility and consistent security across multi-cloud environments as outlined in the "Guide to Cloud Security Posture Management Tools" document.

Reference: https://docs.paloaltonetworks.com/prisma/prisma-cloud/21-04/prisma-cloud-compute- edition-

admin/vulnerability_management/serverless_functions.html

Question: 52

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

Explanation:

"you can also create configuration policies to scan your Infrastructure as Code (IaC) templates that are used to deploy cloud resources. The policies used for scanning IaC templates use a JSON query instead of RQL."

https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/prisma-cloud-policies/create-a-policy

Question: 53

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: D

Explanation:

In Prisma Cloud Enterprise, for alerts to be generated for configuration assets in an onboarded public cloud account, it is essential that the account is associated with an alert rule that matches the enabled config policies. If the account is not linked to an alert rule or if the existing alert rules do not match the config policies, no alerts will be generated even though configuration resource ingestion is visible, and RQL statements return config resource results. This requirement emphasizes the need for a well-structured alerting mechanism to ensure that security incidents are promptly identified and addressed.

Question: 54

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: A

Explanation:

To specifically target running containers with a Cloud Native Application Framework (CNAF) policy in Prisma Cloud, the administrator should scope the policy to Image names. By doing so, the policy will

apply to containers based on the images they were created from, allowing for precise targeting of security policies to specific containers. This approach is part of Prisma Cloud's capabilities to provide granular security controls for

containerized environments, ensuring that policies are effectively applied to the relevant containers.

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

Question: 55

The InfoSec team wants to be notified via email each time a Security Group is misconfigured. Which Prisma Cloud tab should you choose to complete this request?

A. Notifications

B. Policies

C. Alert Rules

D. Events

Answer: C

Explanation:

In Prisma Cloud, to notify the InfoSec team via email about misconfigured Security Groups, the appropriate tab to use is "Alert Rules." Alert rules in Prisma Cloud define the conditions under which alerts are generated and the notification channels, including email, where these alerts are sent. By configuring alert rules related to Security Group misconfigurations, the platform can automatically notify the team when such an event occurs, ensuring prompt awareness and response to potential security issues.

Question: 56

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: B

Explanation:

https://docs.paloaltonetworks.com/prisma/prisma-cloud/22-06/prisma-cloud-compute-edition-admin/install/install_defender/install_host_defender

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

Explanation:

Reference: https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/prisma- cloud-policies/create-a-policy.html

In Prisma Cloud, Config policies have built-in CLI commands for auto-remediation. These policies

help in identifying misconfigurations within cloud environments and can automatically execute remediation commands to correct the configurations without manual intervention. This feature is part of Prisma Cloud's comprehensive approach to maintaining cloud security posture by ensuring that cloud resources are configured in accordance with best practices and compliance standards.

Question: 58

A customer is deploying Defenders to a Fargate environment. It wants to understand the vulnerabilities in the image it is deploying.

How should the customer automate vulnerability scanning for images deployed to Fargate?

A. Set up a vulnerability scanner on the registry

B. Embed a Fargate Defender to automatically scan for vulnerabilities

C. Designate a Fargate Defender to serve a dedicated image scanner

D. Use Cloud Compliance to identify misconfigured AWS accounts

Answer: A

Explanation:

To automate vulnerability scanning for images deployed to Fargate, the customer should set up a vulnerability scanner on the container registry where the images are stored before they are deployed. By scanning the images in the registry, any vulnerabilities can be identified and addressed before the images are used to create Fargate tasks. This proactive approach to vulnerability management is crucial in cloud-native environments to ensure that deployed containers are free from known vulnerabilities.

Reference: https://blog.paloaltonetworks.com/prisma-cloud/securing-aws-fargate-tasks/

Question: 59

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: B

Explanation:

The correct construction for scanning a container image using the TwistCLI tool in Prisma Cloud is option B. This command specifies the address of the Prisma Cloud Console and the image to be scanned, including its tag. The TwistCLI tool is part of Prisma Cloud's capabilities to integrate security into the CI/CD pipeline, allowing for the scanning of images for vulnerabilities as part of the build process, thus ensuring that only secure images are deployed.

Question: 60

DRAG DROP

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	Ordered Options
POST https://api.prismacloud.io/login	
GET https://api.prismacloud.io/report	
GET https://api.prismacloud.io/report/id/download	

Answer:

Explanation:

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

Question: 61

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: B,C

Explanation:

Ensuring that builds can function properly after a Console upgrade in Prisma Cloud involves strategies that maintain compatibility and functionality with the latest versions of the Prisma Cloud tools and services.

Option B: Updating any build environments that have twistcli included to use the latest version is crucial because twistcli is Prisma Cloud's CLI tool used for scanning images, serverless functions, and IaC for vulnerabilities and compliance issues. Ensuring that twistcli is up to date in all build environments guarantees compatibility with the latest features and security definitions provided by Prisma Cloud, as well as ensures that any new or updated policies and checks are accurately enforced during the build process.

Option C: Configuring build pipelines to download twistcli at the start of each build ensures that the most current version of twistcli is used every time a build is initiated. This approach is beneficial in dynamic CI/CD environments where builds are frequent, and maintaining the latest security posture is critical. By downloading twistcli dynamically, teams can automatically adapt to any updates or changes introduced in the Prisma Cloud Console without manual intervention, ensuring seamless integration and continuous compliance with Prisma Cloud's security standards.

Reference:

Prisma Cloud Documentation: Emphasizes the importance of keeping security tools up to date and integrating them into CI/CD pipelines for continuous security.

Best Practices for Integrating Security Tools in CI/CD: Guides on how to effectively incorporate security scanning tools like twistcli into the CI/CD process to ensure builds are secure and compliant.

Question: 62

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: A

Explanation:

1) Select Policies 2) Select the policy rule to edit, on 3 Compliance Standards click + and associate the policy with the compliance standard (https://docs.paloaltonetworks.com/prisma/prisma- cloud/prisma-cloud-admin/prisma-cloud-compliance/create-a-custom-compliance-standard)

Question: 63

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: D

Explanation:

The given admission control policy is designed to evaluate pod creation requests in a Kubernetes environment, specifically targeting the creation of privileged pods, which can pose significant security risks.

Option D: The policy will block the creation of a privileged pod is the correct answer when the effect of the policy is set to “block”. In this context, the policy's logic checks if a pod being created is set to run in privileged mode (a high-risk configuration that grants the pod extended system privileges). If such a configuration is detected, the policy triggers an action to block the pod's creation, thereby preventing the deployment of privileged pods that could undermine the security posture of the

Kubernetes environment.

Reference:

Kubernetes Admission Controllers Documentation: Provides a comprehensive overview of admission controllers in Kubernetes, including how they can be used to enforce policy decisions, such as preventing the creation of

privileged pods.

Best Practices for Kubernetes Security: Discusses the importance of admission control policies in maintaining the security and integrity of Kubernetes environments, with specific emphasis on the risks associated with privileged pods.

Question: 64

Per security requirements, an administrator needs to provide a list of people who are receiving emails 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: D

Explanation:

In Prisma Cloud, the list of people who are receiving e-mails for alerts is managed within the configuration of individual Alert Rules.

Option D: Set Alert Notification section within an Alert Rule is where administrators can specify the e-mail recipients for alerts generated by Prisma Cloud. This section allows for the customization of alert notifications, including the selection of recipients who should receive email notifications when an alert is triggered. This granularity ensures that the right stakeholders are informed about specific security incidents or compliance violations, facilitating timely and appropriate responses.

Reference:

Prisma Cloud Alert Configuration Documentation: Details the process of setting up alert rules in Prisma Cloud, including how to configure notification settings and specify recipients for email alerts.

Alert Management Best Practices: Offers insights into effective alert management strategies, highlighting the importance of targeted alert notifications in ensuring that critical security information reaches the relevant parties promptly.

Question: 65

A customer wants to scan a serverless function as part of a build process. Which twistcli command can be used to scan serverless functions?

A. twistcli function scan <SERVERLESS_FUNCTION.ZIP>

B. twistcli scan serverless <SERVERLESS_FUNCTION.ZIP>

C. twistcli serverless AWS <SERVERLESS_FUNCTION.ZIP>

D. twiscli serverless scan <SERVERLESS_FUNCTION.ZIP>

Answer: D

Explanation:

https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/vulnerability_management/serverless_functions You can also use the twistcli command line utility to scan your serverless functions. First download your serverless function as a ZIP file, then run: $ twistcli serverless scan <SERVERLESS_FUNCTION.ZIP>

Question: 66

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: C

Explanation:

Managing Defender upgrades in a Prisma Cloud environment requires careful planning, especially in scenarios where not all Defenders can be upgraded simultaneously due to maintenance window constraints.

Option 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 is the recommended approach in this situation. This option allows administrators to manually select specific Defenders for upgrade within the available maintenance window, providing control over the upgrade process and ensuring that upgrades are aligned with operational requirements and maintenance schedules.

Reference:

Prisma Cloud Defender Management Documentation: Details the procedures for managing and upgrading Prisma Cloud Defenders, including manual upgrade processes for individual Defenders.

Best Practices for Managing Defender Upgrades: Offers guidelines on effectively planning and executing Defender upgrades, emphasizing the importance of aligning upgrade activities with maintenance windows to minimize disruption to the development environment.

Question: 67

What is an example of an outbound notification within Prisma Cloud?

A. AWS Inspector

B. Qualys

C. Tenable

D. PagerDuty

Answer: D

Explanation:

Outbound notifications in Prisma Cloud refer to the integration with external systems or services for the purpose of alerting or incident management.

Option D: PagerDuty is an example of an outbound notification within Prisma Cloud. PagerDuty is a popular incident response and alerting service that teams use to manage, track, and respond to incidents in real-time. Prisma Cloud's integration with PagerDuty allows organizations to automatically forward alerts from Prisma Cloud to PagerDuty, enabling streamlined incident management and response workflows.

Reference:

Prisma Cloud Integration Documentation: Provides instructions for integrating Prisma Cloud with various external services, including PagerDuty, to enhance alerting and incident management capabilities.

Incident Management Best Practices: Discusses strategies for effective incident management, highlighting the role of integrations with external alerting services like PagerDuty in improving response times and incident resolution.

Question: 68

A security team has been asked to create a custom policy.

Which two methods can the team use to accomplish this goal? (Choose two.)

A. add a new policy

B. clone an existing policy

C. disable an out-of-the-box policy

D. edit the query in the out-of-the-box policy

Answer: A,B

Explanation:

To create a custom policy within a cloud security platform like Prisma Cloud, security teams have the flexibility to either add a new policy from scratch or clone an existing one to serve as a foundation for customization. Adding a new policy allows for the creation of a completely tailored rule set based on specific security requirements. Cloning an existing

policy, on the other hand, provides a quick start by using the structure of an already established policy, which can then be modified to fit particular needs. This approach is beneficial for maintaining consistency with existing policies while addressing unique security scenarios. Disabling an out-of-the-box policy (option C) or editing the query in an out-of-the-box policy (option D) are actions that might be taken to customize policy enforcement but do not equate to the creation of a new custom policy.

Reference: https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/prisma- cloud-policies/manage-prisma-cloud-policies

Question: 69

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: D

Explanation:

The question focuses on valid host compliance policies within a cloud environment. Among the given options, the most relevant to host compliance is ensuring compliant Docker daemon configuration. Docker daemon configurations are critical for securing the host environment where containers are run. A compliant Docker daemon configuration involves setting security-related options to ensure

the Docker engine operates securely. This can include configurations related to TLS for secure communication, logging levels, authorization plugins, and user namespace remapping for isolation.

Ensuring functions are not overly permissive (Option A) and ensuring images are created with a nonroot user (Option C) are more directly related to the security best practices for serverless functions and container images, respectively, rather than host-specific compliance checks. Ensuring host devices are not directly exposed to containers (Option B) is also important for security, but it falls under the broader category of container runtime security rather than host-specific compliance.

Thus, the most valid host compliance policy from the given options is to ensure a compliant Docker daemon configuration, as it directly impacts the security posture of the host environment in a containerized infrastructure. This aligns with best practices for securing Docker environments and is a common recommendation in container security guidelines, including those from Docker and cybersecurity frameworks.

Reference:

Docker Documentation: Security configuration and best practices for Docker engine:

https://docs.docker.com/engine/security/

CIS Docker Benchmark: Providing consensus-based best practices for securing Docker environments:

https://www.cisecurity.org/benchmark/docker/

Question: 70

DRAG DROP

Match the correct scanning mode for each given operation.

(Select your answer from the pull-down list. Answers may be used more than once or not at all.)

Answer Area

Create SNS Topic Triggers	Drag answer here	No data security scan
Select an S3 bucket	Drag answer here	Forward Scan only
Select an S3 bucket with existing files	Drag answer here	Forward or Backward Scan
Link an S3 logging to CloudTrail	Drag answer here	Backward Scan only

Answer:

Explanation:

Create SNS Topic Triggers: No data security scan

Select an S3 bucket: Forward Scan only

Select an S3 bucket with existing files: Forward or Backward Scan

Link an S3 logging to CloudTrail: Backward Scan only

The scanning mode for Data Security in AWS typically depends on the configuration and the desired outcomes for monitoring and protecting data within S3 buckets.

Creating SNS Topic Triggers is a configuration step that does not directly involve scanning. It is part of setting up notifications for events in S3 buckets, but on its own, it does not initiate a data security scan.

Selecting an S3 bucket without specifying existing files typically implies that you intend to scan new objects as they are added to the bucket, which is known as a Forward Scan. This mode is proactive and scans files upon their arrival in the bucket.

When you select an S3 bucket with existing files, you can perform either Forward Scanning for new

files or Backward Scanning to scan all existing files in the bucket. This option provides the most comprehensive scanning coverage for both new and existing data.

Linking an S3 logging to CloudTrail is usually a step taken to monitor access and changes to S3 resources. In the context of scanning, linking S3 to CloudTrail does not initiate a scan, but the CloudTrail logs can be used to trigger a Backward Scan if configured to do so, which scans historical files in the bucket based on CloudTrail events.

Question: 71

A customer wants to be notified about port scanning network activities in their environment. Which policy type detects this behavior?

A. Network

B. Port Scan

C. Anomaly

D. Config

Answer: C

Explanation:

https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/prisma-cloud- policies/anomaly-policies

Question: 72

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

Explanation:

https://docs.paloaltonetworks.com/prisma/prisma-cloud/19-11/prisma-cloud-compute-edition-admin/firewalls/deploy_cnaf

When configuring Cloud Native Application Firewall (CNAF) rules, the specified port should be the one where the container itself listens for web traffic. In this scenario, since the NGINX container is listening on port 8080, the CNAF rule should be configured to protect traffic on port 8080. This ensures that the firewall rule is applied to the traffic intended for the container, regardless of the port mapping on the host.

The documentation from Palo Alto Networks provides guidance on deploying CNAF and specifies that the port in the firewall rule should match the container's listening port, not the host's mapped port. This is an important distinction for properly securing containerized applications with CNAF.

Question: 73

Which three types of buckets exposure are available in the Data Security module? (Choose three.)

A. Public

B. Private

C. International

D. Differential

E. Conditional

Answer: A,B,E

Explanation:

In the Data Security module of cloud security platforms like Prisma Cloud, the types of bucket exposures typically include Public (option A), Private (option B), and Conditional (option E). Public

buckets are accessible by anyone on the internet, posing a significant data leakage risk. Private buckets are restricted to authorized users only, offering a higher level of security. Conditional exposure involves buckets that may be accessible under certain conditions or to specific users, requiring careful configuration and policy enforcement to prevent unauthorized access. International (option C) and Differential (option D) do not represent standard types of bucket exposures in cloud security contexts.

Question: 74

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

Explanation:

https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/audit/audit_admin_activity

Question: 75

DRAG DROP

What is the order of steps to create a custom network policy?

(Drag the steps into the correct order of occurrence, from the first step to the last

www.atmicnetworks.com

Answer Area

Unordered Options	Ordered Options
Build your Query → New Search or Saved Search	
Select Compliance Standards	
From Policies tab → Add Policy → Network	
Click Confirm	

Explanation:

Answer:

Answer Area

Unordered Options	Ordered Options
Build your Query → New Search or Saved Search	From Policies tab → Add Policy → Network
Select Compliance Standards	Build your Query → New Search or Saved Search
From Policies tab → Add Policy → Network	Select Compliance Standards
Click Confirm	Click Confirm

A picture containing table Description automatically generated

Reference:

https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/prisma-cloud-policies/create-a- policy.html

Select Policies and click Add Policy

Build the query

Add the compliance standards

Click Submit.

https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/prisma-cloud-policies/create-a-policy

Question: 76

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

Question: 77

A customer has a large environment that needs to upgrade Console without upgrading all Defenders at one time.

What are two prerequisites prior to performing a rolling upgrade of Defenders? (Choose two.)

A. manual installation of the latest twistcli tool prior to the rolling upgrade

B. all Defenders set in read-only mode before execution of the rolling upgrade

C. a second location where you can install the Console

D. additional workload licenses are required to perform the rolling upgrade

E. an existing Console at version n-1

Answer: A,E

Explanation:

https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/upgrade/upgrade_process_saas After the Console has been upgraded, check and upgrade any of the Defenders that have reached the end of their support lifecycle (Defenders are backward compatible for N-2 releases). The Defender release image is built from the UBI8-minimal base image and on upgrade it is a full container image upgrade, which means that the old Defender container is replaced with a new container. Then, upgrade all other Prisma Cloud components, such as the Jenkins plugin.

Question: 78

An administrator sees that a runtime audit has been generated for a Container. The audit message is "DNS resolution of suspicious name wikipedia.com. type A".

Why would this message appear as an audit?

A. The DNS was not learned as part of the Container model or added to the DNS allow list.

B. This is a DNS known to be a source of malware.

C. The process calling out to this domain was not part of the Container model.

D. The Layer7 firewall detected this as anomalous behavior.

Answer: A

Explanation:

The runtime audit message indicating "DNS resolution of suspicious name wikipedia.com. type A" would appear as an audit because the DNS was not learned as part of the Container model or added to the DNS allow list (option A). In cloud security platforms like Prisma Cloud, runtime protection policies monitor the behavior of running containers and compare it against a learned model of expected behavior. If a container attempts to resolve a DNS name that was not observed during the learning phase or specifically allowed, it triggers an audit event to alert security teams of potentially malicious activity.

Question: 79

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

Explanation:

In the context of Kubernetes, an admission controller is a piece of code that intercepts requests to the Kubernetes API server before the persistence of the object, but after the request is authenticated and authorized. The admission controller lets you apply complex validation and policy controls to objects before they are created or updated.

The ValidatingWebhookConfiguration is a Kubernetes object that tells the API server to send an admission

validation request to a service (the admission webhook) when a request to create, update, or delete a Kubernetes object matches the rules defined in the configuration. The webhook can then approve or deny the request based on custom logic.

The MutatingWebhookConfiguration is similar but is used to modify objects before they are created or updated, which is not the primary function of an admission controller acting in a protective or validating capacity.

DestinationRules are related to Istio service mesh and are not relevant to Kubernetes admission control.

PodSecurityPolicies (PSPs) are a type of admission controller in Kubernetes but they are predefined by Kubernetes and do not require a specific configuration object like ValidatingWebhookConfiguration. PSPs are also deprecated in recent versions of Kubernetes.

Therefore, the correct answer is C. ValidatingWebhookConfiguration, as it is the Kubernetes object used to configure admission webhooks for validating requests, which aligns with the role of Defender acting as an admission controller in Prisma Cloud.

Reference from the provided documents:

The documents uploaded do not contain specific details about Kubernetes objects or Prisma Cloud's integration with Kubernetes. However, this explanation aligns with general Kubernetes practices and Prisma Cloud's capabilities in securing Kubernetes environments.

Reference: https://docs.paloaltonetworks.com/prisma/prisma-cloud/21-04/prisma-cloud-compute-edition- admin/access_control/open_policy_agent.html

Question: 80

Which three options are selectable in a CI policy for image scanning with Jenkins or twistcli? (Choose three.)

A. Scope - Scans run on a particular host

B. Credential

C. Apply rule only when vendor fixes are available

D. Failure threshold

E. Grace Period

Answer: A,C,D

Explanation:

https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/continuous_integration/set_policy_ci_plugins

Question: 81

Which component(s), if any, will Palo Alto Networks host and run when a customer purchases Prisma Cloud Enterprise Edition?

A. Defenders

B. Console

C. Jenkins

D. twistcli

Answer: B

Explanation:

In Prisma Cloud Enterprise Edition, Palo Alto Networks hosts and runs the Console component. The Console serves as the central management interface for Prisma Cloud, allowing customers to configure policies, view alerts, and manage their cloud security posture without the need to host this component themselves.

Question: 82

Which port should a security team use to pull data from Console's API?

A. 53

B. 25

C. 8084

D. 8083

Answer: D

Explanation:

Both Console's API and web interfaces, served on port 8083 (HTTPS), require authentication over a different channel with different credentials (e.g. username and password, access key, and so on), none of which Defender holds. https://docs.paloaltonetworks.com/prisma/prisma-cloud/22- 06/prisma-cloud-compute-edition-admin/technology_overviews/defender_architecture

Question: 83

You are an existing customer of Prisma Cloud Enterprise. You want to onboard a public cloud account and immediately see all of the alerts associated with this account based off ALL of your tenant's existing enabled policies. There is no requirement to send alerts from this account to a downstream application at this time.

Which option shows the steps required during the alert rule creation process to achieve this objective?

A. Ensure the public cloud account is assigned to an account group Assign the confirmed account group to alert ruleSelect "select all policies" checkbox as part of the alert rule Confirm the alert rule

B. Ensure the public cloud account is assigned to an account group Assign the confirmed account group to alert ruleSelect one or more policies checkbox as part of the alert rule Confirm the alert rule

C. Ensure the public cloud account is assigned to an account group Assign the confirmed account group to alert ruleSelect one or more policies as part of the alert rule Add alert notificationsConfirm the alert rule

D. Ensure the public cloud account is assigned to an account group Assign the confirmed account group to alert ruleSelect "select all policies" checkbox as part of the alert rule Add alert notificationsConfirm the alert rule

Answer: A

Explanation:

To immediately see all alerts associated with a newly onboarded public cloud account based on existing enabled policies, it is essential to assign the account to an account group and then create an alert rule that applies to this account group. By selecting "select all policies," the alert rule will trigger alerts for all existing enabled policies without the need to specify individual policies or add alert notifications for downstream applications.

Question: 84

A customer has configured the JIT, and the user created by the process is trying to log in to the Prisma Cloud console. The user encounters the following error message:

What is the reason for the error message?

A. The attribute name is not set correctly in JIT settings.

B. The user does not exist.

C. The user entered an incorrect password

D. The role is not assigned for the user.

Answer: A

Explanation:

Reference:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CmZ4CAK

The error message encountered by the user trying to log into the Prisma Cloud console is likely due to an incorrect configuration in the Just-In-Time (JIT) settings, specifically the attribute name used for JIT authentication. This could prevent the user from being recognized correctly by the Prisma Cloud console.

Question: 85

What are the two ways to scope a CI policy for image scanning? (Choose two.)

A. container name

B. image name

C. hostname

D. image labels

Answer: B,D

Explanation:

Reference: https://www.optiv.com/insights/source-zero/blog/defending-against-container-threats- palo-alto-prisma-cloud

In Prisma Cloud, CI policies for image scanning can be scoped based on the image name and image labels. These scoping options allow for targeted scanning of images, ensuring that policies are applied to relevant images based on their identifiers or metadata.

Question: 86

Which policy type in Prisma Cloud can protect against malware?

A. Data

B. Config

C. Network

D. Event

Answer: A

Explanation:

Reference: https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/prisma- cloud-policies/create-a-policy.html#:~:text=%E2%80%94Data%20policies%20protect%20against%20malware,for%20Data%20Exposure%20or%20Malware

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.

Question: 87

If you are required to run in an air-gapped environment, which product should you install?

A. Prisma Cloud Jenkins Plugin

B. Prisma Cloud Compute Edition

C. Prisma Cloud with self-hosted plugin

D. Prisma Cloud Enterprise Edition

Answer: B

Explanation:

Reference: https://docs.paloaltonetworks.com/prisma/prisma-cloud.html

Prisma Cloud Compute Edition is the suitable product for air-gapped environments, where there is no direct internet access. This edition can be installed and operated in isolated environments, providing cloud security capabilities without the need for external connectivity.

Question: 88

What is the maximum number of access keys a user can generate in Prisma Cloud with a System Admin role?

A. 1

B. 2

C. 3

D. 4

Answer: B

Explanation:

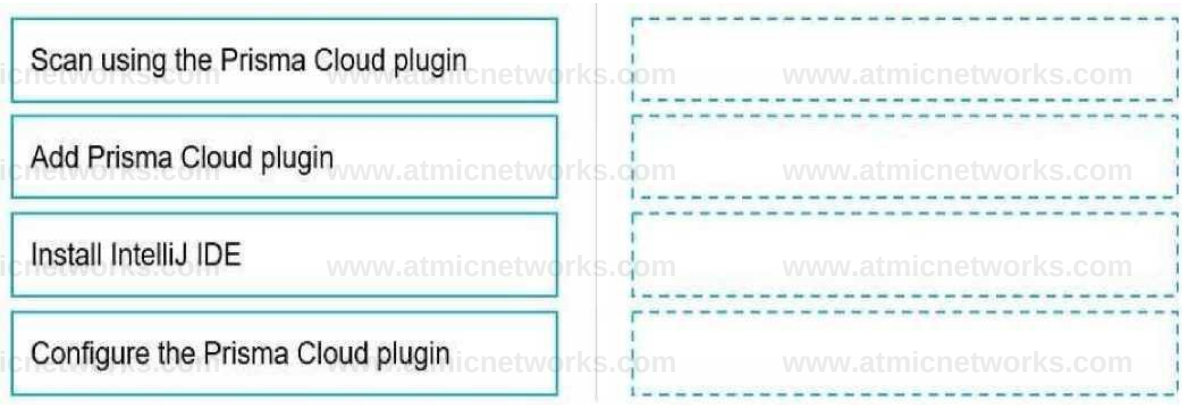
Reference: https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/manage-prisma-cloud-administrators/create-access-keys.html#:~:text=You%20can%20enable%20API%20access,generate%20one%20access%20key%20only

In Prisma Cloud, a user with a System Admin role can generate a maximum of 2 access keys. These keys are used for API access and automation, enabling secure and controlled interactions with Prisma Cloud's capabilities.

Question: 89

DRAG DROP

Put the steps involved to configure and scan using the IntelliJ plugin in the correct order.



Explanation:

Answer:

Install IntelliJ IDE

Add Prisma Cloud plugin

Configure the Prisma Cloud plugin

Scan using the Prisma Cloud plugin

To configure and use the Prisma Cloud plugin for scanning within the IntelliJ Integrated Development Environment (IDE), you must follow a series of steps in a specific order to ensure proper setup and functionality.

Firstly, you need to have the IntelliJ IDE installed on your system. Without the IDE, you cannot add or use the Prisma Cloud plugin, as it is designed to work within this development environment.

Secondly, after installing the IntelliJ IDE, you add the Prisma Cloud plugin. This involves navigating to the plugin marketplace within IntelliJ and selecting the Prisma Cloud plugin for installation.

Once the plugin is added to your IntelliJ IDE, the next step is to configure the Prisma Cloud plugin. This configuration may include setting up your Prisma Cloud credentials, specifying your scan options, and other settings that tailor the plugin's functionality to your needs.

Finally, after the plugin is installed and configured, you can proceed to scan your project using the Prisma Cloud plugin. This will check your code against security policies and compliance standards, providing feedback and recommendations for any identified issues.

Following these steps ensures that the Prisma Cloud plugin is properly integrated into your IntelliJ development workflow, allowing for continuous security and compliance checks as part of the development process.

Question: 90

An administrator needs to detect and alert on any activities performed by a root account.

Which policy type should be used?

A. config-run

B. config-build

C. network

D. audit event

Answer: D

Explanation:

To detect and alert on activities performed by a root account, an audit event policy should be used. An audit event policy is a type of policy that can be used to detect suspicious activities or events that may be related to security threats. This type of policy will allow the administrator to monitor and alert on any activities performed by a root account.

https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/prisma-cloud-policies/prisma-cloud-threat-detection

The correct policy type to use in order to detect and alert on any activities performed by a root account is an "audit event" policy. An audit event policy is designed to monitor and record a series of chronological events in the order they occur, typically used to track user activities and changes within the system. When a root account performs any actions, an audit event policy will log these events, allowing the administrator to review and potentially set up alerts if suspicious or unauthorized activities are detected. This type of policy is crucial for security and compliance purposes as it helps ensure that all actions performed with root privileges are legitimate and authorized.

Reference to this can be found in most cloud security platforms that offer CSPM (Cloud Security Posture Management) solutions. For example, within Prisma Cloud by Palo Alto Networks, audit events are a part of the Activity Monitoring features, which track user activities and system changes to facilitate investigations into suspicious or unauthorized actions.

Question: 92

A customer has multiple violations in the environment including:

User namespace is enabled

An LDAP server is enabled

SSH root is enabled

Which section of Console should the administrator use to review these findings?

A. Manage

B. Vulnerabilities

C. Radar

D. Compliance

Answer: D

Explanation:

The correct section of the Console that the administrator should use to review findings such as "User namespace is enabled", "An LDAP server is enabled", and "SSH root is enabled" is "Compliance".

The "Compliance" section in CSPM tools like Prisma Cloud provides an overview of the current compliance posture against various regulatory standards and best practices. It can help identify configurations that do not adhere to best practices or that may violate compliance requirements, such as enabling the user namespace, which could be a security risk, or having an LDAP server and SSH root enabled, which may not comply with certain security standards.

Reference to the use of the "Compliance" section can be found in CSPM documentation, where it

details how compliance checks are used to assess the security and configuration of cloud resources against established benchmarks and standards, allowing organizations to maintain compliance and improve their security posture.

Question: 93

A customer has serverless functions that are deployed in multiple clouds.

Which serverless cloud provider is covered be “overly permissive service access” compliance check?

A. Alibaba

B. GCP

C. AWS

D. Azure

Answer: C

Explanation:

Reference: https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/compliance/serverless.html

The serverless cloud provider covered by the “overly permissive service access” compliance check is AWS (Amazon Web Services). AWS Lambda, which is the serverless computing platform provided by AWS, may have functions that are assigned more permissions than they require to perform their operations, leading to security risks.

In the context of CSPM tools, such as Prisma Cloud, checks for overly permissive service access would typically include examining the policies attached to AWS Lambda functions to ensure that they adhere to the principle of least privilege. Such checks help identify and rectify overly broad permissions that could potentially be exploited by

attackers.

The reference for this can be found in AWS best practices for Lambda security, which emphasize the importance of granting minimal privileges necessary for the Lambda function to perform its tasks, thereby reducing the potential attack surface.

Question: 94

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?

A. 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.

B. Set www.evil-url.com as a blocklisted DNS name in the default Container runtime policy, and set the effect to block.

C. Choose "copy into rule" for any Container, set www.evil-url.com as a blocklisted DNS name, and set the effect to prevent.

D. Set www.evil-url.com as a blocklisted DNS name in the default Container policy and set the effect to prevent.

Answer: D

Explanation:

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

www.atmicnetworks.com

Question: 95

Which API calls can scan an image named myimage: latest with twistcli and then retrieve the results from Console?

A. $ twistcli images scan \--address \--user \--password \--verbose \myimage: latest

B. $ twistcli images scan \--address \--user \--password \--details \myimage: latest

C. $ twistcli images scan \--address \--user \--password \myimage: latest

D. $ twistcli images scan \--address \--user \--password \--console \myimage: latest

Answer: B

Explanation:

You can have twistcli generate a detailed report for each scan. The following procedure shows you how to scan an image with twistcli, and then retrieve the results from Console.

https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin- compute/tools/twistcli_scan_images

Question: 96

Given the following RQL:

event from cloud.audit_logs where operation IN ('CreateCryptoKey', 'DestroyCryptoKeyVersion', 'v1.compute.disks.createSnapshot')

Which audit event snippet is identified?

A)

"request": { "resource": "604173093072", "@type": "type.googleapis.com/google.iani.vl.SetlamPolicyRequest", "policy": ("bindings": [

B)

C)

www.atmicnetworks.com

{ "Statement": [{ "Action": "*", "Effect": "Allow", "Resource": "*" }], "Version": "2012-10-17"

D)

"payload": ("requestMetadata": ("callerSuppliedUserAgent": "Terraform/0.14.0
(+https: 7/ww. terraform.io) Terrafom-Plugin-SDK/2.1.0 terraform-provider-google/3.50.0, gz.ip (gfe) ", "callerip": "34.265.226.252"], "request":
{ "@type":
"type.googleapis.com/compute.disks.treateSnapshot" },

A. Option A

B. Option B

C. Option C

D. Option D

Answer: D

Explanation:

https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-rql-reference/rql- reference/event-query/event-query-examples

Question: 97

Which two of the following are required to be entered on the IdP side when setting up SSO in Prisma Cloud? (Choose two.)

A. Username

B. SSO Certificate

C. Assertion Consumer Service (ACS) URL

D. SP (Service Provider) Entity ID

Answer: C,D

Explanation:

When setting up Single Sign-On (SSO) in Prisma Cloud on the Identity Provider (IdP) side, it is essential to configure the

Assertion Consumer Service (ACS) URL and the Service Provider (SP) Entity ID. The ACS URL is the endpoint to which the IdP will send the SAML assertion, and the SP Entity ID is a unique identifier for the service provider that often resembles a URL but does not necessarily point to a location. These elements are crucial for establishing the trust relationship between the IdP and the service provider, enabling secure user authentication and authorization.

Question: 98

An administrator sees that a runtime audit has been generated for a container.

The audit message is:

"/bin/ls launched and is explicitly blocked in the runtime rule. Full command: ls -latr"

Which protection in the runtime rule would cause this audit?

A. Networking

B. File systems

C. Processes

D. Container

Answer: C

Explanation:

The protection in the runtime rule that would cause the audit message indicating "/bin/ls launched and is explicitly blocked in the runtime rule" is related to "Processes". In container security, a runtime rule set to monitor and restrict processes can block specific executables or commands from running within a container. If the rule is triggered, it indicates that a process that is explicitly denied by the policy attempted to execute, which in this case is the 'ls' command.

https://docs.paloaltonetworks.com/prisma/prisma-cloud/22-12/prisma-cloud-compute-edition-admin/runtime_defense/runtime_audits

Question: 99

Which data security default policy is able to scan for vulnerabilities?

A. Objects containing Vulnerabilities

B. Objects containing Threats

C. Objects containing Malware

D. Objects containing Exploits

Answer: C

Explanation:

The data security default policy capable of scanning for vulnerabilities is "Objects containing Malware". In cloud security, malware scanning is an essential feature of CSPM tools that allows for the identification of malicious software within objects stored in the cloud. A policy that scans for objects containing malware ensures that any files or code bases in the cloud environment are examined for potential threats, protecting the cloud resources from being compromised.

Explanation:

Question: 101

Which three fields are mandatory when authenticating the Prisma Cloud plugin in the IntelliJ application? (Choose three.)

A. Secret Key

B. Prisma Cloud API URL

C. Tags

D. Access Key

E. Asset Name

Answer: A,B,D

Explanation:

Reference: https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/prisma- cloud-devops-security/use-the-prisma-cloud-plugin-for-intellij.html

When authenticating the Prisma Cloud plugin in the IntelliJ application, the mandatory fields are the Secret Key, Prisma Cloud API URL, and Access Key. These credentials are required to securely authenticate and enable the plugin to communicate with the Prisma Cloud API, ensuring that the plugin can perform its intended functions within the development environment.

Question: 102

Which of the following are correct statements regarding the use of access keys? (Choose two.)

A. Access keys must have an expiration date

B. Up to two access keys can be active at any time

C. System Admin can create access key for all users

D. Access keys are used for API calls

Answer: B,D

Explanation:

Regarding the use of access keys, it is correct that up to two access keys can be active at any time for a single IAM user in AWS, and access keys are used for programmatic API calls to AWS services. This allows for rotation of keys without immediate invalidation of the old key and ensures secure access

to AWS services via APIs.

Question: 104

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?

A. The development team should create a WAAS rule for the host where these pods will be running.

B. The development team should create a WAAS rule targeted at all resources on the host.

C. The development team should create a runtime policy with networking protections.

D. The development team should create a WAAS rule targeted at the image name of the pods.

Answer: D

Explanation:

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

Question: 105

A manager informs the SOC that one or more RDS instances have been compromised and the SOC needs to make sure production RDS instances are NOT publicly accessible.

Which action should the SOC take to follow security best practices?

A. Enable "AWS S3 bucket is publicly accessible" policy and manually remediate each alert.

B. Enable "AWS RDS database instance is publicly accessible" policy and for each alert, check that it is a production instance, and then manually remediate.

C. Enable "AWS S3 bucket is publicly accessible" policy and add policy to an auto-remediation alert rule.

D. Enable "AWS RDS database instance is publicly accessible" policy and add policy to an autoremediation alert rule.

Answer: B

Explanation:

Following best practices, the Security Operations Center (SOC) should enable a policy that checks for publicly accessible AWS RDS database instances and then manually remediate each instance confirmed to be part of the production environment. This approach ensures that only those resources that should not be publicly accessible are modified, avoiding unintended access restrictions on non-production instances.

Question: 106

An administrator wants to enforce a rate limit for users not being able to post five (5) .tar.gz files within five (5) seconds.

What does the administrator need to configure?

A. A ban for DoS protection with an average rate of 5 and file extensions match on .tar.gz on WAAS

B. A ban for DoS protection with a burst rate of 5 andfile extensions match on .tar.gz on CNNF

C. A ban for DoS protection with a burst rate of 5 and file extensions match on .tar gz on WAAS

D. A ban for DoS protection with an average rate of 5 and file extensions match on .tar.gz on CNNF

Answer: C

Explanation:

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

Question: 107

What is an automatically correlated set of individual events generated by the firewall and runtime sensors to identify unfolding attacks?

A. policy

B. incident

C. audit

D. anomaly

Answer: B

Explanation:

Reference: https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/runtime_defense/incident_explorer.html

An automatically correlated set of individual events generated by the firewall and runtime sensors to identify unfolding attacks is known as an "incident". Incidents provide a consolidated view of related security events, making it easier for administrators to understand the scope and potential impact of an attack, and to take appropriate response actions.

Question: 108

A customer wants to monitor the company's AWS accounts via Prisma Cloud, but only needs the resource configuration to be monitored for now.

Which two pieces of information do you need to onboard this account? (Choose two.)

A. Cloudtrail

B. Subscription ID

C. Active Directory ID

D. External ID

E. Role ARN

Answer: A,E

Explanation:

To onboard an AWS account into Prisma Cloud for the purpose of monitoring resource configurations, the necessary information includes the Role ARN (Amazon Resource Name) and CloudTrail setup. The Role ARN (Option E) is crucial because Prisma Cloud requires permission to access and monitor resources within the AWS account, which is facilitated through an IAM role that Prisma Cloud can assume. This IAM role must have the necessary permissions to access AWS services and resources that Prisma Cloud needs to monitor. CloudTrail (Option A) is essential for auditing and monitoring API calls within the AWS environment, including those related to resource configurations. It provides visibility into user and resource activity by recording API calls made on the account.

CloudTrail logs are used by Prisma Cloud to detect changes in resource configurations and ensure compliance with security policies. Subscription ID (Option B) and Active Directory ID (Option C) are more relevant to Azure cloud environments, not AWS. External ID (Option D) is used in a crossaccount role trust relationship to prevent the "confused deputy" problem, but it's not specifically required just to onboard the account for resource configuration monitoring.

Question: 109

An administrator for Prisma Cloud needs to obtain a graphical view to monitor all connections, including connections across hosts and connections to any configured network objects.

Which setting does the administrator enable or configure to accomplish this task?

A. ADEM

B. WAAS Analytics

C. Telemetry

D. Cloud Native Network Firewall

E. Host Insight

Answer: D

Explanation:

Reference: https://docs.paloaltonetworks.com/prisma/prisma-cloud/21-04/prisma-cloud-compute- edition-admin/firewalls/cnnf_self_hosted.html

To obtain a graphical view to monitor all connections, including those across hosts and to configured network objects within Prisma Cloud, the appropriate feature to enable or configure is the Cloud Native Network Firewall (Option D). Prisma Cloud's Cloud Native Network Firewall provides visibility into network traffic and allows for the monitoring and control of network flows within the cloud environment, effectively enabling administrators to visualize and secure inter-host communications and connections to network objects. ADEM (Option A) and WAAS Analytics (Option B) are not related to Prisma Cloud's capabilities for monitoring connections. Telemetry (Option C) involves the collection of data and metrics but does not specifically provide a graphical view of connections. Host Insight (Option E) focuses on providing visibility into host-related activities and vulnerabilities but does not specifically deal with monitoring network connections in the graphical manner described.

Question: 110

Which two fields are required to configure SSO in Prisma Cloud? (Choose two.)

A. Prisma Cloud Access SAML URL

B. Identity Provider Issuer

C. Certificate

D. Identity Provider Logout URL

Answer: B,C

Explanation:

Configuring Single Sign-On (SSO) in Prisma Cloud requires the Identity Provider Issuer (Option B) and Certificate (Option C). The Identity Provider Issuer is a unique identifier for the SSO identity provider and is used by Prisma Cloud to establish trust and validate SSO responses. The Certificate, typically an X.509 certificate, is used to sign SSO assertions and ensure the security of the SSO communication. The Prisma Cloud Access SAML URL (Option A) is provided by Prisma Cloud to configure the SSO on the identity provider's side, not the other way around. The Identity Provider Logout URL (Option D) is used for single logout configurations but is not a required field for basic SSO configuration in Prisma Cloud.

Question: 111

Which two IDE plugins are supported by Prisma Cloud as part of its DevOps Security? (Choose two.)

A. BitBucket

B. Visual Studio Code

C. CircleCI

D. IntelliJ

Answer: B,D

Explanation:

Prisma Cloud supports integration with various Integrated Development Environments (IDEs) as part of its DevOps Security offerings, including Visual Studio Code (Option B) and IntelliJ (Option D). These integrations allow developers to scan their Infrastructure as Code (IaC) templates and application code for vulnerabilities and compliance issues directly within their preferred development

environments, promoting a "shift left" security approach. BitBucket (Option A) and CircleCI (Option C) are more commonly associated with Continuous Integration/Continuous Deployment (CI/CD) pipelines rather than being IDEs.

Question: 112

Which two CI/CD plugins are supported by Prisma Cloud as part of its DevOps Security? (Choose two.).

A. BitBucket

B. Visual Studio Code

C. CircleCI

D. IntelliJ

Answer: A,C

Explanation:

For CI/CD plugins supported by Prisma Cloud as part of its DevOps Security, BitBucket (Option A) and CircleCI (Option C) are the correct choices. BitBucket is widely used for source code management and collaboration, while CircleCI is a popular CI/CD platform. Prisma Cloud integrates with these tools to scan code repositories and CI/CD pipelines for security issues, ensuring that vulnerabilities are identified and addressed early in the development process. Visual Studio Code (Option B) and IntelliJ (Option D) are IDEs rather than CI/CD tools, and while they are supported by Prisma Cloud for scanning and security purposes, they are not considered CI/CD plugins.

Question: 113

Given the following JSON query:

$.resource[*].aws_s3_bucket exists

Which tab is the correct place to add the JSON query when creating a Config policy?

A. Details

B. Compliance Standards

C. Remediation

D. Build Your Rule (Run tab)

E. Build Your Rule (Build tab)

Answer: E

Explanation:

F. When creating a Config policy in Prisma Cloud and incorporating a JSON query, the correct place to add this query is under the "Build Your Rule (Build tab)" (Option E). This section allows users to define the criteria and conditions for the policy, including specifying JSON or RQL (Resource Query Language) queries that articulate the policy's logic. The "Details" (Option A) tab is typically used for general information about the policy, such as its name and description. The "Compliance Standards" (Option B) tab is for associating the policy with specific compliance frameworks. The "Remediation" (Option C) tab provides guidance on how to remediate any issues detected by the policy. The "Build Your Rule (Run tab)" (Option D) is not a standard option in Prisma Cloud policy configuration

.

Question: 114

Which two attributes of policies can be fetched using API? (Choose two.)

A. policy label

B. policy signature

C. policy mode

D. policy violation

Answer: A,C

Explanation:

Using the Prisma Cloud API, users can fetch various attributes of policies, including the policy label (Option A) and policy mode (Option C). The policy label helps in categorizing and organizing policies, while the policy mode determines how the policy is enforced (e.g., alert, enforce). The policy signature (Option B) is not a standard attribute exposed via the API for fetching, as it relates more to the internal identification and handling of policies. The policy violation (Option D) is an outcome or event resulting from a policy breach, not an attribute of the policy itself that can be fetched via the API.

Question: 115

Which two options may be used to upgrade the Defenders with a Console v20.04 and Kubernetes deployment? (Choose two.)

A. Run the provided curl | bash script from Console to remove Defenders, and then use Cloud Discovery to automatically redeploy Defenders.

B. Remove Defenders DaemonSet, and then use Cloud Discovery to automatically redeploy the Defenders.

C. Remove Defenders, and then deploy the new DaemonSet so Defenders do not have to automatically update on each deployment.

D. Let Defenders automatically upgrade.

Answer: C,D

Explanation:

For upgrading Defenders with a Console v20.04 and Kubernetes deployment, the following two options are viable:

C . Remove Defenders, and then deploy the new DaemonSet: This option involves manually removing the existing Defenders and then deploying a new DaemonSet. This method ensures that the Defenders are updated to the latest version without relying on automatic updates12.

D . Let Defenders automatically upgrade: Prisma Cloud provides the capability for Defenders to automatically upgrade themselves. This feature simplifies the upgrade process by eliminating the need for manual intervention3.

Both methods are supported and can be used depending on the organization's policies and preferences regarding Defender upgrades. The automatic upgrade feature is particularly useful for maintaining up-to-date security without manual oversight, while the manual removal and redeployment of a new DaemonSet can be preferred in environments where more control over the upgrade process is desired123.

Question: 116

DRAG DROP

Move the steps to the correct order to set up and execute a serverless scan using AWS DevOps.

Answer:

Explanation:

Download Prisma Cloud Lambda function executable	First
Create Lambda function with settings	Second
Create a pipeline with settings	Third
Execute Pipeline	Fourth

Graphical user interface, text, application Description automatically generated

Question: 117

A customer has a requirement to scan serverless functions for vulnerabilities.

What is the correct option to configure scanning?

A. Configure serverless radar from the Defend > Compliance > Cloud Platforms page.

B. Embed serverless Defender into the function.

C. Configure a function scan policy from the Defend > Vulnerabilities > Functions page.

D. Use Lambda layers to deploy a Defender into the function.

Answer: C

Explanation:

In Prisma Cloud, the capability to scan serverless functions, such as AWS Lambda functions, for vulnerabilities is an integral

part of ensuring cloud security posture management (CSPM) and compliance. Specifically, option C is correct because Prisma Cloud provides a dedicated section for defining policies related to serverless function vulnerabilities under the "Defend > Vulnerabilities > Functions" page. This feature allows administrators to create and manage policies that automatically scan serverless functions for known vulnerabilities, ensuring that the functions comply with the organization's security standards before they are deployed. This approach aligns with Prisma Cloud's comprehensive security model that covers various aspects of cloud security, including serverless functions, as outlined in the "Guide to Cloud Security Posture Management Tools" document

https://docs.paloaltonetworks.com/prisma/prisma-cloud/22-12/prisma-cloud-compute-edition-admin/vulnerability_management/serverless_functions

Question: 118

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?

A. Prisma Cloud Administrator's Guide (Compute)

B. Prisma Cloud API Reference

C. Prisma Cloud Compute API Reference

D. Prisma Cloud Enterprise Administrator's Guide

Answer: B

Explanation:

Prisma Cloud has a REST API that enables you to access Prisma Cloud features programmatically.

Most actions supported on the Prisma Cloud web interface are available with the REST API, refer to the Prisma Cloud REST API Reference for details about the REST API. https://pan.dev/prisma- cloud/api/cspm/

For scripting and programmatically querying user data and associated permission levels in a Prisma Cloud Enterprise tenant, the Prisma Cloud API Reference is the most relevant documentation. This reference guide provides detailed information on the available APIs, including those for user and permissions management. It outlines the necessary attributes, endpoints, and methods required to programmatically interact with the Prisma Cloud platform.

The API Reference is designed to help developers and administrators understand how to leverage the Prisma Cloud APIs to automate tasks, such as querying existing users and their permission levels. It includes examples and explanations that are

crucial for writing effective scripts that integrate with the Prisma Cloud infrastructure.

While the Administrator's Guides provide valuable information on managing the platform, the API Reference is specifically tailored for developers looking to automate and script interactions with Prisma Cloud services. Therefore, reviewing the Prisma Cloud API Reference will provide the necessary details to fulfill the DevSecOps team's requirement1.

Question: 119

When would a policy apply if the policy is set under Defend > Vulnerability > Images > Deployed?

A. when a serverless repository is scanned

B. when a Container is started form an Image

C. when the Image is built and when a Container is started form an Image

D. when the Image is built

Answer: B

Explanation:

In Prisma Cloud, policies set under "Defend > Vulnerability > Images > Deployed" are specifically designed to apply at runtime, i.e., when a container is instantiated from an image. This ensures that any image, regardless of its point of origin or creation time, is evaluated against the defined vulnerability policies at the time it is deployed as a container in the environment. This runtime enforcement is crucial for catching vulnerabilities that may not have been present or detected during

the image build phase, providing an additional layer of security for running applications.

https://docs.paloaltonetworks.com/prisma/prisma-cloud/22-12/prisma-cloud-compute-edition-admin/vulnerability_management/vuln_management_rules

Question: 120

Which two required request headers interface with Prisma Cloud API? (Choose two.)

A. Content-type:application/json

B. x-redlock-auth

C. >x-redlock-request-id

D. Content-type:application/xml

Answer: A,B

Explanation:

Reference: https://prisma.pan.dev/api/cloud/api-headers/

Interfacing with the Prisma Cloud API, especially for tasks such as automation, integration, and advanced querying, requires specific request headers for authentication and data format specification. "Content-type:application/json" is essential for indicating that the request body is formatted as JSON, which is a widely accepted data interchange format. The "x-redlock-auth" header is critical for passing the API access key or token, which authenticates the request to Prisma Cloud's API. This authentication mechanism ensures secure access to Prisma Cloud's capabilities while maintaining the integrity and confidentiality of the interactions.

Question: 121

An administrator has a requirement to ingest all Console and Defender logs to Splunk.

Which option will satisfy this requirement in Prisma Cloud Compute?

A. Enable the API settings for logging.

B. Enable the CSV export in the Console.

C. Enable the syslog option in the Console

D. Enable the Splunk option in the Console.

Answer: C

Explanation:

Log into Console. / Go to Manage > Alerts > Logging. / Configure Prisma Cloud to send audit event records to syslog, stdout and Prometheus.

https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin- compute/audit/logging

To ingest all Console and Defender logs into Splunk within Prisma Cloud Compute, the most effective method is to enable the syslog option in the Console. This configuration allows the direct export of logs in a format compatible with Splunk, facilitating real-time log analysis and monitoring. This setup supports continuous security monitoring and advanced threat detection capabilities by utilizing Splunk's extensive data processing and visualization tools.

Question: 122

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 ofline.

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

Question: 123

During an initial deployment of Prisma Cloud Compute, the customer sees vulnerabilities in their environment.

Which statement correctly describes the default vulnerability policy?

A. It blocks all containers that contain a vulnerability.

B. It alerts on any container with more than three critical vulnerabilities.

C. It blocks containers after 30 days if they contain a critical vulnerability.

D. It alerts on all vulnerabilities, regardless of severity.

Answer: D

Explanation:

By default, Prisma Cloud's vulnerability policy is configured to alert on all detected vulnerabilities across containers and images, without filtering based on the severity of the vulnerabilities. This default setting ensures that administrators are made aware of all potential security issues, providing them with comprehensive visibility into the security posture of their

environment. Administrators can then assess and prioritize these vulnerabilities based on their context, severity, and impact on the organization's assets.

Question: 124

Console is running in a Kubernetes cluster, and you need to deploy Defenders on nodes within this cluster.

Which option shows the steps to deploy the Defenders in Kubernetes using the default Console service name?

A. From the deployment page in Console, choose pod name for Console identifier, generate DaemonSet file, and apply the DaemonSet to twistlock namespace.

B. From the deployment page configure the cloud credential in Console and allow cloud discovery to auto-protect the Kubernetes nodes.

C. From the deployment page in Console, choose twistlock-console for Console identifier, generate

DaemonSet file, and apply DaemonSet to the twistlock namespace.

D. From the deployment page in Console, choose twistlock-console for Console identifier, and run the curl | bash script on the master Kubernetes node.

Answer: C

Explanation:

Reference: https://cdn.twistlock.com/docs/downloads/Twistlock-Reference-Architecture.pdf

Deploying Defenders in a Kubernetes cluster involves generating a DaemonSet configuration from the Prisma Cloud Console. The "twistlock-console" is typically used as the Console identifier, which facilitates the communication between the Defenders and the Console. The generated DaemonSet file is then applied to the Kubernetes cluster, specifically within the "twistlock" namespace, ensuring that a Defender is deployed on each node within the cluster for comprehensive protection. This method is in line with Kubernetes best practices for deploying cluster-wide agents, ensuring seamless and scalable deployment of Prisma Cloud's security capabilities.

Question: 125

Which RQL query type is invalid?

A. Event

B. IAM

C. Incident

D. Config

Answer: C

Explanation:

Within Prisma Cloud's Resource Query Language (RQL), the "Incident" query type is invalid because RQL is designed to query configuration and posture information of cloud resources, not incident data. The valid RQL query types include "Config" for querying resource configurations, "Network" for querying network-related information, "IAM" for querying identity and access management configurations, and "Event" for querying audit events. The focus on resource configurations and audit events aligns with Prisma Cloud's capabilities in cloud security posture management (CSPM) and

cloud workload protection platform (CWPP), providing insights into resource configurations, compliance, and network traffic.Top of Form

Bottom of Form

Question: 126

On which cloud service providers can you receive new API release information for Prisma Cloud?

A. AWS, Azure, GCP, Oracle, IBM

B. AWS, Azure, GCP, Oracle, Alibaba

C. AWS, Azure, GCP, IBM

D. AWS, Azure, GCP, IBM, Alibaba

Answer: B

Explanation:

Prisma Cloud, developed by Palo Alto Networks, is known for its comprehensive cloud security capabilities across various cloud service providers (CSPs). The integration and support extend to major CSPs, including AWS (Amazon Web Services), Azure (Microsoft's Cloud), GCP (Google Cloud Platform), Oracle Cloud, and Alibaba Cloud. This wide range of support ensures that organizations leveraging multi-cloud environments can maintain consistent security postures across all their cloud assets. The information regarding supported CSPs by Prisma Cloud can typically be found in their official

documentation and release notes, which detail the features, integrations, and enhancements specific to each CSP.

Question: 127

Web-Application and API Security (WAAS) provides protection for which two protocols? (Choose two.)

A. HTTP

B. SSH

C. Tomcat Web Connector via AJP

D. TLS

Answer: A,D

Explanation:

Web-Application and API Security (WAAS) is a feature within Prisma Cloud that focuses on protecting web applications and APIs from various threats and vulnerabilities. The primary protocols it provides protection for are HTTP (Hypertext Transfer Protocol) and TLS (Transport Layer Security). HTTP is the foundation of data communication for the World Wide Web, and TLS is a cryptographic protocol designed to provide communications security over a computer network. While SSH (Secure Shell) is a protocol for secure remote login and other secure network services, and Tomcat Web Connector via AJP (Apache JServ Protocol) is used for Tomcat server communication, they are not the primary focus of WAAS protection.

Question: 128

What is the most reliable and extensive source for documentation on Prisma Cloud APIs?

A. prisma.pan.dev

B. docs.paloaltonetworks.com

C. Prisma Cloud Administrator's Guide

D. Live Community

Answer: A

Explanation:

Prisma Cloud's API documentation and extensive developer resources are primarily hosted on prisma.pan.dev, which is Palo Alto Networks' developer portal. This site offers comprehensive guides, API references, and resources for developers to integrate, automate, and extend the capabilities of Prisma Cloud within their applications and workflows. While docs.paloaltonetworks.com provides official product documentation, and Prisma Cloud Administrator's Guide offers in-depth administrative guidance, prisma.pan.dev is specifically designed to serve as the hub for API documentation and developer resources. The Live Community is another valuable resource for peer support and discussions but is not the primary source for API documentation.

https://prisma.pan.dev/api/cloud/

Question: 129

How often do Defenders share logs with Console?

A. Every 10 minutes

B. Every 30 minutes

C. Every 1 hour

D. Real time

Answer: D

Explanation:

In Prisma Cloud, Defenders play a crucial role in securing cloud environments by monitoring and protecting workloads. The communication between Defenders and the Prisma Cloud Console occurs in real-time, allowing for immediate detection of threats, vulnerabilities, and compliance issues. This real-time communication is essential for maintaining an up-to-date security posture and promptly responding to potential security incidents. The real-time nature of Defender-Console communication ensures that security teams have the latest information and can take swift actions to mitigate risks.

Question: 130

In Prisma Cloud Software Release 22.06 (Kepler), which Registry type is added?

A. Azure Container Registry

B. Google Artifact Registry

C. IBM Cloud Container Registry

D. Sonatype Nexus

Answer: B

Explanation:

In the Prisma Cloud Software Release 22.06, referred to as the Kepler release, the addition of Google Artifact Registry as a supported Registry type was a significant update. Google Artifact Registry is designed to store, manage, and secure your container images and language packages (such as Maven and npm). It provides a single place for teams to manage their artifacts and dependencies, improving consistency and security across software development and deployment processes. This update in Prisma Cloud reflects the platform's commitment to supporting the latest cloud-native technologies and services, enhancing its capabilities in securing modern cloud environments.

Question: 131

Which three elements are part of SSH Events in Host Observations? (Choose three.)

A. Startup process

B. User

C. System calls

D. Process path

E. Command

Answer: B,D,E

Explanation:

SSH Events in Host Observations within Prisma Cloud focus on activities related to Secure Shell (SSH) usage, which is critical for secure communication and remote management of cloud resources. The elements that are part of SSH Events include the User involved in the SSH session, the Process path that indicates the executable or command invoked during the session, and the Command itself that was executed. These elements are crucial for security monitoring and forensic analysis as they provide detailed context about SSH activities, helping security teams to identify unauthorized access, potential breaches, or malicious activities within their cloud environments. Startup process and System calls, while important in other contexts, are not directly associated with SSH Events in Host Observations.

Question: 132

Which two variables must be modified to achieve automatic remediation for identity and access management (IAM) alerts in Azure cloud? (Choose two.)

A. API ENDPOINT

B. SQS_QUEUE_NAME

C. SB_QUEUE_KEY

D. YOUR_ACCOUNT_NUMBER

Answer: A,C

Explanation:

AZURE:

% export SB_QUEUE_KEY=your_sb_queue_key

% export SB_QUEUE_KEY_NAME=your_sb_queue_key_name

% export SB_QUEUE_NAME_SPACE=your_sb_queue_name_space

% export API_ENDPOINT=api_tenant

% export AUTH_KEY=your_jwt_token

https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/prisma-cloud-iam-security/remediate-alerts-for-iam-security

Question: 133

Which three actions are required in order to use the automated method within Azure Cloud to streamline the process of using remediation in the identity and access management (IAM) module? (Choose three.)

A. Install boto3 & requests library.

B. Configure IAM Azure remediation script.

C. Integrate with Azure Service Bus.

D. Configure IAM AWS remediation script.

E. Install azure.servicebus & requests library.

Answer: B,C,E

Explanation:

To use the automated method within Azure Cloud for streamlining the process of using remediation in the identity and access management (IAM) module, the required actions include configuring the IAM Azure remediation script, integrating with Azure Service Bus, and installing the azure.servicebus & requests library. These steps ensure that the automated remediation system can communicate effectively with Azure services, execute the necessary remediation actions, and address IAM-related alerts by adjusting permissions and access controls as needed. This automation helps maintain a secure and compliant cloud environment by promptly addressing potential IAM issues.

https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/prisma-cloud-iam-security/remediate-alerts-for-iam-security

Question: 134

Which two roles have access to view the Prisma Cloud policies? (Choose two.)

A. Build AND Deploy Security

B. Auditor

C. Dev SecOps

D. Defender Manager

Answer: B,C

Explanation:

In Prisma Cloud, roles with access to view policies include Auditor and Dev SecOps. The Auditor role is typically focused on compliance and oversight, allowing users to review configurations, policies, and compliance status without making changes. The Dev SecOps role bridges the gap between development, security, and operations, focusing on integrating security practices within the CI/CD pipeline. Both roles require access to Prisma Cloud policies to perform their functions effectively, ensuring that security and compliance are maintained throughout the cloud environment and application lifecycle.

Question: 135

An administrator has added a Cloud account on Prisma Cloud and then deleted it.

What will happen if the deleted account is added back on Prisma Cloud within a 24-hour period?

A. No alerts will be displayed.

B. Existing alerts will be displayed again.

C. New alerts will be generated.

D. Existing alerts will be marked as resolved.

Answer: B

Explanation:

When an administrator adds a Cloud account to Prisma Cloud and then deletes it, if the deleted account is added back to Prisma Cloud within a 24-hour period, the existing alerts associated with that account will be displayed again. This behavior ensures continuity in monitoring and alerting, allowing security teams to retain visibility into potential security issues or compliance violations associated with the cloud account. Re-displaying existing alerts helps maintain a consistent security posture and ensures that no critical alerts are overlooked during the re-addition process.

https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/manage-prisma- cloud-alerts/view-respond-to-prisma-cloud-alerts

Question: 136

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

A. Pull the images from the Prisma Cloud registry without any authentication.

B. Authenticate with Prisma Cloud registry, and then pull the images from the Prisma Cloud registry.

C. Retrieve Prisma Cloud images using URL auth by embedding an access token.

D. Download Prisma Cloud images from github.paloaltonetworks.com.

Answer: B,C

Explanation:

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.

www.atmicnetworks.com

Question: 137

Which action would be applicable after enabling anomalous compute provisioning?

A. It detects the activity caused by the spambot.

B. It detects unusual server port activity or unusual protocol activity from a client within or outside the cloud environment.

C. It detects potential creation of an unauthorized network of compute instances with AutoFocus.

D. It detects potential creation of an unauthorized network of compute instances either accidentally or for cryptojacking.

Answer: D

Explanation:

Enabling anomalous compute provisioning in Prisma Cloud allows for the detection of unusual and potentially unauthorized activities related to the creation of compute instances. This feature is particularly useful for identifying scenarios where an unauthorized network of compute instances might be established, either accidentally due to misconfigurations or maliciously for purposes such as cryptojacking. Cryptojacking involves the unauthorized use of someone else's compute resources to mine cryptocurrency, and anomalous compute provisioning can help in identifying such activities by highlighting unusual patterns in the provisioning of compute resources.

Question: 138

What is the function of the external ID when onboarding a new Amazon Web Services (AWS) account in Prisma Cloud?

A. It is a unique identifier needed only when Monitor & Protect mode is selected.

B. It is the resource name for the Prisma Cloud Role.

C. It is a UUID that establishes a trust relationship between the Prisma Cloud account and the AWS account in order to extract data.

D. It is the default name of the PrismaCloudApp stack.

Answer: C

Explanation:

The external ID plays a crucial role when onboarding a new Amazon Web Services (AWS) account in Prisma Cloud. It serves as a UUID (Universally Unique Identifier) that establishes a trust relationship between the Prisma Cloud account and the AWS account. This trust relationship is essential for allowing Prisma Cloud to securely extract data and perform security monitoring and compliance checks within the AWS environment. The use of an external ID ensures that Prisma Cloud can access the necessary information from the AWS account without compromising the security of the AWS account's credentials, adhering to the principle of least privilege and enhancing the overall security posture.

Question: 139

Which IAM Azure RQL query would correctly generate an output to view users who have sufficient permissions to create security groups within Azure AD and create applications?

A. config where api.name = 'azure-active-directory-authorization-policy' AND json.rule = defaultUserRolePermissions.allowedToCreateSecurityGroups is true and defaultUserRolePermissions.allowedToCreateApps is true

B. config from cloud.resource where api.name = 'azure-active-directory-authorization-policy' AND json.rule = defaultUserRolePermissions exists

C. config from network where api.name = 'azure-active-directory-authorization-policy' AND json.rule = defaultUserRolePermissions.allowedToCreateSecurityGroups is false and defaultUserRolePermissions.allowedToCreateApps is true

D. config from cloud.resource where api.name = 'azure-active-directory-authorization-policy' AND json.rule = defaultUserRolePermissions.allowedToCreateSecurityGroups is true and defaultUserRolePermissions.allowedToCreateApps is true

Answer: D

Explanation:

The correct RQL query to view users who have sufficient permissions to create security groups within Azure AD and create applications is option D. This query is specifically designed to assess policies within Azure Active Directory (Azure AD) by checking the authorization policy settings related to user default role permissions. The query targets the azure-active-directory-authorization-policy API to fetch configurations (config from cloud.resource) and then filters those configurations based on the JSON rules that dictate whether users are allowed to create security groups (defaultUserRolePermissions.allowedToCreateSecurityGroups is true) and applications (defaultUserRolePermissions.allowedToCreateApps is true). This query provides a comprehensive check by ensuring both conditions are met, which is necessary for users to have the combined capabilities of creating security groups and applications within Azure AD.

In the context of Prisma Cloud and cloud security principles, the RQL (Resource Query Language) is utilized for querying the configuration state of resources within cloud environments to ensure compliance with security policies. The RQL syntax in option D precisely aligns with the requirements for identifying users with specific permissions, leveraging

Prisma Cloud's capability to provide visibility and control over cloud resources, as emphasized in various resources like the "Prisma Cloud Visibility and Control Qualification Guide" and the "Guide to Cloud Security Posture Management Tools." These documents highlight the importance of continuous monitoring and validation of cloud resource configurations to maintain a secure and compliant cloud environment, which is effectively achieved through targeted RQL queries like the one in option D.

Reference:

"Prisma Cloud Visibility and Control Qualification Guide" discusses the importance of visibility and compliance in cloud environments, which is directly applicable to the use of RQL for querying resource configurations.

"Guide to Cloud Security Posture Management Tools" emphasizes the need for comprehensive visibility and governance across cloud environments, further supporting the rationale behind the specific RQL query used to assess user permissions in Azure AD.

Question: 140

Which two bot types are part of Web Application and API Security (WAAS) bot protection? (Choose two.)

A. Chat bots

B. User-defined bots

C. Unknown bots

D. Customer bots

Answer: B,C

Explanation:

Web Application and API Security (WAAS) bot protection within the Prisma Cloud ecosystem includes various types of bots, with "User-defined bots" and "Unknown bots" being two key categories. User- defined bots refer to bots that organizations have explicitly identified and categorized based on their behavior and purpose. These can include legitimate bots such as search engine crawlers or internal automation tools, which are recognized and allowed based on predefined criteria set by the user.

Unknown bots, on the other hand, encompass bots that have not been explicitly identified or categorized by the user or the system. These can potentially include malicious bots that attempt to scrape data, perform DDoS attacks, or exploit vulnerabilities in web applications and APIs. The categorization of unknown bots is crucial for maintaining security, as it allows for the monitoring and analysis of bot behavior to identify potential threats and take appropriate actions.

In the context of Prisma Cloud and its emphasis on securing cloud-native applications, the differentiation between user-defined and unknown bots is significant. Prisma Cloud's approach to WAAS bot protection is designed to provide granular

control over bot traffic, enabling organizations to distinguish between beneficial and harmful bot activities. This aligns with the broader goal of ensuring the security and integrity of web applications and APIs in a cloud environment, as highlighted in documents such as the "Prisma-Cloud-Visibility-and-Control-Qualification-Guide" and "Guide-to-CSPM-Tools-Email-Social -LP-Copy." These resources emphasize the importance of comprehensive security measures that include the management of bot traffic to protect against a wide range of web-based threats.

Reference:

"Prisma-Cloud-Visibility-and-Control-Qualification-Guide" discusses the importance of visibility and control in cloud environments, including the management of bot traffic as part of a comprehensive security strategy.

"Guide-to-CSPM-Tools-Email-Social -LP-Copy" highlights the need for advanced security tools and practices, such as WAAS bot protection, to manage and mitigate the risks associated with web applications and APIs in the cloud.

Question: 141

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.)

A. Install boto3 & requests library.

B. Configure IAM Azure remediation script.

C. Integrate with Azure Service Bus.

D. Configure IAM AWS remediation script.

Answer: A,D

Explanation:

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."

Reference:

"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.

Question: 142

Which three public cloud providers are supported for VM image scanning? (Choose three.)

A. GCP

B. Alibaba

C. Oracle

D. AWS

E. Azure

Answer: A,D,E

Explanation:

VM image scanning is a critical component of cloud security, allowing organizations to identify vulnerabilities within virtual machine images before deployment. The three major public cloud providers supported for VM image scanning are Google Cloud Platform (GCP), Amazon Web Services (AWS), and Microsoft Azure. These platforms offer extensive infrastructure services and are commonly used in various industries, making them primary targets for VM image scanning integration.

GCP, AWS, and Azure each provide capabilities to store, manage, and deploy VM images through their respective services such as Google Compute Engine, AWS EC2, and Azure Virtual Machines. By integrating VM image scanning with these services, organizations can ensure that their VM images are free from known vulnerabilities and comply with security best practices before being deployed in the cloud environment.

This approach to VM image scanning is consistent with Prisma Cloud's comprehensive security strategy, which

emphasizes the importance of securing cloud workloads across the entire development lifecycle. By supporting VM image scanning across GCP, AWS, and Azure, Prisma Cloud enables organizations to maintain a consistent security posture across multiple cloud environments, mitigating the risk of deploying vulnerable or misconfigured VM images that could lead to security breaches.

Reference:

Documentation from GCP, AWS, and Azure on VM management and security best practices provide foundational knowledge for understanding how VM image scanning integrates with each cloud provider's infrastructure services.

Prisma Cloud's documentation and best practices guides offer insights into how VM image scanning is implemented within its security platform to protect cloud workloads across GCP, AWS, and Azure.

Question: 143

Where can Defender debug logs be viewed? (Choose two.)

A. /var/lib/twistlock/defender.log

B. From the Console, Manage > Defenders > Manage > Defenders. Select the Defender from the deployed Defenders list, then click Actions > Logs

C. From the Console, Manage > Defenders > Deploy > Defenders. Select the Defender from the deployed Defenders list, then click Actions > Logs

D. /var/lib/twistlock/log/defender.log

Answer: B,D

Explanation:

In Prisma Cloud, Defender debug logs are essential for troubleshooting and understanding the Defender's operational behavior. The logs can be accessed through two primary methods:

A . The first method (B) involves using the Prisma Cloud Console's user interface. By navigating to Manage > Defenders > Manage > Defenders, administrators can select a deployed Defender from the list and access its logs by clicking Actions > Logs. This method provides a convenient way to view logs directly from the Console without the need to access the Defender host directly.

D . The second method (D) involves accessing the logs directly from the file system of the host where the Defender is deployed. The correct path for the Defender logs is /var/lib/twistlock/log/defender.log. This method is useful for situations where direct access to the host is available, and it allows for more in-depth troubleshooting by examining the raw log files.

Options A and C are incorrect because the paths and navigation steps provided do not accurately reflect the structure and functionality of Prisma Cloud's logging system.

Question: 144

How many CLI remediation commands can be added in a custom policy sequence?

A. 2

B. 1

C. 4

D. 5

Answer: D

Explanation:

You can define up to 5 CLI commands in a sequence for a multi-step automatic remediation workflow. Add the commands in the sequence you want them to execute and separate the commands with a semi colon. If any CLI command included in the sequence fails, the execution stops at that point.

The Prisma Cloud platform allows administrators to define up to 5 CLI commands in a sequence for a multi-step automatic remediation workflow. These commands should be added in the order they are intended to be executed and must be separated by a semicolon. If any CLI command in the sequence fails during execution, the process stops at that point. This feature enables administrators to automate the remediation process efficiently and effectively, ensuring that actions are taken in a specific order to address alerts or compliance issues.

This capability is detailed in the Prisma Cloud documentation under the section for configuring Prisma Cloud to automatically remediate alerts. It's an important feature for maintaining security and compliance in cloud environments, as it allows for quick and automated responses to identified issues.

Question: 145

An administrator wants to retrieve the compliance policies for images scanned in a continuous integration (CI) pipeline.

Which endpoint will successfully execute to enable access to the images via API?

A. GET /api/v22.01/policies/compliance

B. GET /api/v22.01/policies/compliance/ci

C. GET /api/v22.01/policies/compliance/ci/images

D. GET /api/v22.01/policies/compliance/ci/serverless

Answer: C

Explanation:

The following curl command creates a single rule compliance policy for container images scanned in the CI pipeline: curl 'https://<CONSOLE>/api/v<VERSION>/policies/compliance/ci/images' \

Question: 146

The attempted bytes count displays?

A. traffic that is either denied by the security group or firewall rules or traffic that was reset by a host or virtual machine that received the packet and responded with a RST packet.

B. traffic that is either denied by the security group or firewall rules.

C. traffic that is either denied by the firewall rules or traffic that was reset by a host or virtual machine that received the packet and responded with a RST packet.

D. traffic denied by the security group or traffic that was reset by a host or virtual machine that received the packet and responded with a RST packet.

Answer: A

Explanation:

The attempted bytes count in Prisma Cloud's context refers to the amount of traffic that is either denied by security group or firewall rules, or the traffic that was reset by a host or virtual machine (VM) that received the packet and responded with a RST (Reset) packet (A). This metric is crucial for understanding the nature of blocked or interrupted traffic within the cloud environment, helping administrators identify potential security threats or misconfigurations that may be preventing legitimate traffic. It encompasses both the traffic actively blocked by security controls and the traffic that the receiving entity deemed invalid or unwanted, thus providing a comprehensive view of the network's defensive posture.

Question: 147

Anomaly policy uses which two logs to identify unusual network and user activity? (Choose two.)

A. Network flow

B. Audit

C. Traffic

D. Users

Answer: A,B

Explanation:

Anomaly policies in Prisma Cloud utilize Network flow logs (A) and Audit logs (B) to identify unusual network and user activities. Network flow logs provide visibility into the traffic flow across the network, helping detect anomalies in communication patterns that might indicate malicious activities or network misconfigurations. Audit logs record user actions within the system, offering insights into potentially unauthorized or suspicious operations that could compromise security. By analyzing these logs, anomaly policies can effectively pinpoint irregularities that deviate from established baselines, enabling timely detection and response to potential security threats.

Question: 148

What are two alarm types that are registered after alarms are enabled? (Choose two.)

A. Onboarded Cloud Accounts status

B. Resource status

C. Compute resources

D. External integrations status

Answer: A,D

Explanation:

Upon enabling alarms in Prisma Cloud, two critical alarm types that are registered are Onboarded Cloud Accounts status (A) and External integrations status (D). These alarms are pivotal for maintaining the health and security of the cloud environment. The Onboarded Cloud Accounts status

alarms alert administrators about the connectivity and health of cloud accounts integrated with Prisma Cloud, ensuring continuous monitoring and security coverage. The External integrations status alarms provide notifications regarding the operational status of third-party services and tools integrated with Prisma Cloud, such as SIEMs, ticketing systems, or

other security tools, ensuring that these integrations function correctly to support comprehensive security and incident response workflows.

Question: 149

What is the correct method for ensuring key-sensitive data related to SSNs and credit card numbers cannot be viewed in Dashboard > Data view during investigations?

A. Go to Settings > Data > Snippet Masking and select Full Mask.

B. Go to Settings > Data > Data Patterns, search for SSN Pattern, edit it, and modify the proximity keywords.

C. Go to Settings > Cloud Accounts > Edit Cloud Account > Assign Account Group and select a group with limited permissions.

D. Go to Policies > Data > Clone > Modify Objects containing Financial Information publicly exposed and change the file exposure to Private.

Answer: A

Explanation:

To ensure that sensitive data such as SSNs and credit card numbers are not visible in Dashboard > Data view during investigations, the correct method is to go to Settings > Data > Snippet Masking and select Full Mask (A). This feature in Prisma Cloud allows administrators to mask sensitive data snippets within the dashboard, ensuring that such information is obfuscated and not exposed to unauthorized viewers. Full Masking provides a robust level of protection by completely hiding the sensitive values, thereby enhancing data privacy and compliance with regulations that mandate the protection of personal and financial information.

Question: 150

Which two integrations enable ingesting host findings to generate alerts? (Choose two.)

A. Splunk

B. Tenable

C. JIRA

D. Qualys

Answer: B,D

Explanation:

To ingest host findings and generate alerts in Prisma Cloud, integrations with Tenable (B) and Qualys (D) are supported. These integrations allow Prisma Cloud to ingest vulnerability and compliance data from Tenable and Qualys, which are renowned vulnerability management solutions. By integrating these tools, Prisma Cloud can enhance its visibility into the security posture of hosts within the cloud environment, enabling more comprehensive threat detection and response capabilities. The integration facilitates the aggregation and correlation of findings from these external sources, enriching the overall security intelligence and enabling more informed and timely decision-making regarding threat mitigation and compliance management.

https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/configure-external- integrations-on-prisma-cloud/integrations-feature-support

Question: 151

Which data storage type is supported by Prisma Cloud Data Security?

A. IBM Cloud Object Storage

B. AWS S3 buckets

C. Oracle Object Storage

D. Google storage class

Answer: B

Explanation:

Prisma Cloud Data Security supports various data storage types, including AWS S3 buckets (B). AWS S3 (Simple Storage Service) is a widely used object storage service that offers scalability, data availability, security, and performance. Prisma Cloud's ability to secure S3 buckets is crucial for

organizations leveraging AWS for storage needs, as it ensures that data stored within these buckets is protected against unauthorized access, data breaches, and other security threats. Prisma Cloud provides comprehensive visibility into the data stored in S3 buckets, enabling data classification, compliance monitoring, and threat detection to safeguard sensitive data effectively.

Question: 152

Which action must be taken to enable a user to interact programmatically with the Prisma Cloud APIs and for a nonhuman entity to be enabled for the access keys?

A. Create a role with System Admin and generate access keys.

B. Create a user with a role that has minimal access.

C. Create a role with Account Group Read Only and assign it to the user.

D. Create a role and assign it to the Service Account.

Answer: D

Explanation:

To enable a user to interact programmatically with Prisma Cloud APIs and for a nonhuman entity to access keys, the correct action is to create a role and assign it to the Service Account (D). Service accounts in Prisma Cloud are designed for programmatic access by applications or automated tools, allowing these entities to interact with Prisma Cloud APIs securely. By creating a specific role with the necessary permissions and assigning it to a service account, administrators can ensure that the entity has the appropriate level of access required for its operations, aligning with the principle of least privilege and enhancing the security posture of API interactions.

Question: 153

Which three types of runtime rules can be created? (Choose three.)

A. Processes

B. Network-outgoing

C. Filesystem

D. Kubernetes-audit

E. Waas-request

Answer: A,B,C

Explanation:

In Prisma Cloud, runtime rules are created to monitor and control the behavior of applications and services during their execution to ensure compliance with security policies. The three types of runtime rules that can be created in Prisma Cloud are:

Processes: These rules monitor and control the execution of processes within the environment. They can be used to detect unauthorized or malicious processes and take actions such as alerting, blocking, or terminating the processes.

Network-outgoing: These rules govern the outbound network connections from the applications or containers. They help in controlling access to external resources, preventing data exfiltration, and ensuring that the communication complies with the security policies.

Filesystem: Filesystem rules are related to the access and modification of the file system by applications or containers. These rules can help in detecting unauthorized access, changes to sensitive files, and ensuring that the applications adhere to the least privilege principle in terms of file access.

These runtime rules are essential for maintaining the security and integrity of applications running in cloud environments, especially in dynamic and distributed architectures where traditional perimeterbased security controls may not be sufficient.

Question: 154

Who can access saved searches in a cloud account?

A. Administrators

B. Users who can access the tenant

C. Creators

D. All users with whom the saved search has been shared

Answer: A

Explanation:

Saved Searches has list of search queries saved by any Prisma Cloud administrator.

https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/manage-prisma- cloud-administrators/prisma-cloud-admin-permissions

According to the official Palo Alto Networks documentation, saved searches in a cloud account are managed by administrators. This aligns with the principle that administrative privileges are typically required to manage access to saved searches and other similar resources within cloud platforms. Administrators have the capability to control who can access various resources, ensuring that only authorized users can view or modify saved searches. This is a common security measure to prevent unauthorized access and potential data breaches.

Question: 155

The Compute Console has recently been upgraded, and the administrator plans to delay upgrading the Defenders and the Twistcli tool until some of the team's resources have been rescaled. The Console is currently one major release ahead.

What will happen as a result of the Console upgrade?

A. Defenders will disconnect, and Twistcli will stop working.

B. Defenders will disconnect, and Twistcli will remain working.

C. Both Defenders and Twistcli will remain working.

D. Defenders will remain connected, and Twistcli will stop working.

Answer: C

Explanation:

When the Compute Console in Prisma Cloud is upgraded to a newer major release, while the Defenders and the Twistcli tool remain on the older version, the system is designed to ensure backward compatibility to a certain extent. As a result, both Defenders and Twistcli will continue to operate despite the version discrepancy. The Defenders will remain connected, continuing their monitoring and protection duties, and the Twistcli tool will keep functioning, allowing for continued scanning and other CLI-based operations. This design ensures that the security and functionality of the environment are not abruptly interrupted due to the upgrade process, providing administrators with a window to plan and execute the upgrade of Defenders and Twistcli without immediate pressure.

Question: 156

What are two key requirements for integrating Okta with Prisma Cloud when multiple Amazon Web Services (AWS) cloud accounts are being used? (Choose two.)

A. Super Administrator permissions

B. A valid subscription for the IAM security module

C. An Okta API token for the primary AWS account

D. Multiple instances of the Okta app

Answer: B,D

Explanation:

https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/prisma-cloud-iam- security/integrate-prisma-cloud-with-okta

Question: 157

Which resource and policy type are used to calculate AWS Net Effective Permissions? (Choose two.)

A. Service Linked Roles

B. Lambda Function

C. Amazon Resource Names (ARNs) using Wild Cards

D. AWS Service Control Policies (SCPs)

Answer: B,D

Explanation:

"The list of AWS policy types and identities that are used to calculate the net effective permissions are as follows:

AWS IAM role

AWS IAM policy

AWS IAM group

AWS service control policies (SCPs)

Role trust relationships

Permission boundaries

NotAction

Policies with wild card support

If your cloud environment has additional resource types, Prisma Cloud does not factor them into the net-effective permissions.

In addition, permissions can also be set by a resource-based policy. The following AWS resourcebased policies are

supported in the net effective permissions calculation:

Lambda function

S3 bucket

SQS queue

SNS topic

ECS task definition

Secret manager

KMS key

Lambda layer version"

Question: 158

When an alert notification from the alarm center is deleted, how many hours will a similar alarm be suppressed by default?

A. 12

B. 8

C. 24

D. 4

Answer: C

Explanation:

Click Delete if you want to remove the notification from the alarm center. Once deleted, a similar alarm will not appear for the next 24 hours, if the same error occurs in that time period. After 24 hours, a similar error will generate a new alarm notification.

https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/manage-prisma- cloud-alarms/review-alarms

Question: 159

Which component of a Kubernetes setup can approve, modify, or reject administrative requests?

A. Kube Controller

B. Terraform Controller

C. Admission Controller

D. Control plane

Answer: C

Explanation:

In a Kubernetes environment, the Admission Controller is a critical component responsible for approving, modifying, or rejecting administrative requests before they are processed by the Kubernetes API server. The Admission Controller acts as a gatekeeper, enforcing governance and policy controls by evaluating requests against a set of predefined rules and policies. It can validate and mutate requests, ensuring that only compliant and authorized changes are allowed to proceed. This capability is vital for maintaining the security and integrity of the Kubernetes cluster, as it can prevent unauthorized or potentially harmful actions from being executed, thus playing a key role in the cluster's overall security posture.

Question: 160

Which three actions are available for the container image scanning compliance rule? (Choose three.)

A. Allow

B. Snooze

C. Block

D. Ignore

E. Alert

Answer: C,D,E

Explanation:

The Prisma Cloud documentation specifies the actions that can be taken for container image scanning compliance rules as:

C . Block: This action prevents the use of a container image if it fails to meet the defined compliance criteria.

D . Ignore: This action allows the image to bypass the compliance check, effectively overlooking the identified issues.

E . Alert: This action triggers an alert to notify the relevant stakeholders about the compliance status of the container image.

These actions are integral to Prisma Cloud's governance capabilities, allowing organizations to enforce their security and compliance policies effectively. By setting up these rules, teams can ensure that only images that comply with their standards are deployed, while also having the flexibility to ignore certain images or receive alerts for further investigation.

https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/compliance/trusted_images

Question: 161

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

A. Agentless scan will automatically be disabled, so Defender scans are the only scans occurring.

B. Agentless scans do not conflict with Defender scans, so both will run.

C. Defender scans will automatically be disabled, so agentless scans are the only scans occurring.

D. Both agentless and Defender scans will be disabled and an error message will be received.

Answer: B

Explanation:

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/onboard-accounts

Question: 162

An administrator of Prisma Cloud wants to enable role-based access control for Docker engine.

Which configuration step is needed first to accomplish this task?

A. Configure Docker's authentication sequence to first use an identity provider and then Console.

B. Set Defender's listener type to TCP.

C. Set Docker's listener type to TCP.

D. Configure Defender's authentication sequence to first use an identity provider and then Console.

Answer: B

Explanation:

https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/access_control/rbac

Question: 163

Which of the below actions would indicate – "The timestamp on the compliance dashboard?

A. indicates the most recent data

B. indicates the most recent alert generated

C. indicates when the data was ingested

D. indicates when the data was aggregated for the results displayed

Answer: D

Explanation:

The timestamp on the compliance dashboard in a cloud security context typically reflects the point in time when data from various sources is collected, processed, and then consolidated to present the compliance status or results. This aggregation process involves compiling data from multiple scans, logs, and other compliance-related information to provide a comprehensive overview of the current compliance posture. Therefore, the timestamp usually indicates when this aggregation was completed, ensuring that users are viewing the most up-to-date and relevant compliance information based on the latest data compilation.

Question: 164

During the Learning phase of the Container Runtime Model, Prisma Cloud enters a "dry run" period for how many hours?

A. 4

B. 48

C. 1

D. 24

Answer: D

Explanation:

Learning mode is the phase in which Prisma Cloud performs either static or dynamic analysis. Because the model depends on behavioral inputs, images stay in learning mode for 1 hour to complete the model. After this 1 hour, Prisma Cloud enters a 'dry run' period for 24 hours to ensure there are no behavioral changes and the model is complete. If during these 24 hours, behavioral changes are observed, the model goes back to Learning mode for an additional 24 hours.

Question: 165

Which three incident types will be reflected in the Incident Explorer section of Runtime Defense? (Choose three.)

A. Crypto miners

B. Brute Force

C. Cross-Site Scripting

D. Port Scanning

E. SQL Injection

Answer: A,B,D

Explanation:

This section describes the incident types surfaced in Incident Explorer.

Altered binary

Backdoor admin accounts

Backdoor SSH access

Brute force

Crypto miners

Execution flow hijack attempt

Kubernetes attack

Lateral movement

Malware

Port scanning

Reverse shell

Suspicious binary

https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/runtime_defense/incident_types

Question: 166

Which two filters are available in the SecOps dashboard? (Choose two.)

A. Time range

B. Account Groups

C. Service Name

D. Cloud Region

Answer: A,B

Explanation:

In the SecOps dashboard of a cloud security platform like Prisma Cloud, filters such as Time range and Account Groups are essential for narrowing down the data or security alerts based on specific time periods or organizational structures. The Time range filter allows users to view incidents or compliance data for a particular timeframe, facilitating trend analysis and focusing on recent events. The Account Groups filter enables the segregation of data based on different cloud accounts or organizational units, making it easier for security teams to manage and prioritize security tasks according to the business structure or cloud architecture.

Question: 167

Under which tactic is “Exploit Public-Facing Application” categorized in the ATT&CK framework?

A. Defense Evasion

B. Initial Access

C. Execution

D. Privilege Escalation

Answer: B

Explanation:

In the MITRE ATT&CK framework, the tactic "Exploit Public-Facing Application" is categorized under Initial Access. This tactic involves leveraging vulnerabilities in public-facing applications to gain unauthorized access to an organization's external services or applications. Initial Access tactics are concerned with the methods adversaries use to gain an initial foothold within a network, and exploiting public-facing applications is a common approach used by attackers to breach external defenses and establish a presence within a target network.

Question: 168

Which alert deposition severity must be chosen to generate low and high severity alerts in the Anomaly settings when user wants to report on an unknown browser and OS, impossible time travel, or both due to account hijacking attempts?

A. High

B. Aggressive

C. Moderate

D. Conservative

Answer: B

Explanation:

Aggressive: For unusual user activity—Report on either unknown location or service, or both to classify an anomaly. For account hijacking—Report on unknown browser and Operating System, impossible time travel, or both. For anomalous compute provisioning activity—Reports on low and higher severity alerts.

Question: 169

A user from an organization is unable to log in to Prisma Cloud Console after having logged in the previous day.

Which area on the Console will provide input on this issue?

A. SSO

B. Audit Logs

C. Users & Groups

D. Access Control

Answer: B

Explanation:

In the event a user is unable to log in to the Prisma Cloud Console, Audit Logs serve as a critical area for investigating the issue. Audit Logs provide a detailed record of activities, including login attempts, within the Prisma Cloud environment. By examining the Audit Logs, administrators can identify failed login attempts, understand the reasons behind login failures (e.g., incorrect credentials, account lockouts, or access policy changes), and take appropriate actions to resolve the login issues, ensuring users can access the console as expected.

Question: 170

What happens when a role is deleted in Prisma Cloud?

A. The access key associated with that role is automatically deleted.

B. Any integrations that use the access key to make calls to Prisma Cloud will stop working.

C. The users associated with that role will be deleted.

D. Any user who uses that key will be deleted.

Answer: A

Explanation:

When you create an access key, the key is tied to the role with which you logged in and if you delete the role, the access

key is automatically deleted. https://docs.paloaltonetworks.com/prisma/prisma- cloud/prisma-cloud-admin/manage-prisma-cloud-administrators/create-access-keys

Question: 171

What is the default namespace created by Defender DaemonSet during deployment?

A. Redlock

B. Defender

C. Twistlock

D. Default

Answer: C

Explanation:

the default when using the script is twistlock, but you can use whatever you want. https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/configure/set_diff_paths_daemon_sets

Question: 172

Which three OWASP protections are part of Prisma Cloud Web-Application and API Security (WAAS) rule? (Choose three.)

A. DoS Protection

B. Local file inclusion

C. SQL injection

D. Suspicious binary

E. Shellshock

Answer: B,C,E

Explanation:

In the Prisma Cloud Web-Application and API Security (WAAS) rules, protections against OWASP- recognized

vulnerabilities like Local file inclusion, SQL injection, and Shellshock are included. Local

file inclusion involves unauthorized access to files on the server, potentially leading to sensitive information disclosure. SQL injection targets data-driven applications by inserting malicious SQL statements into an entry field, while Shellshock exploits vulnerabilities in Bash, a widely used Unix shell, to execute arbitrary commands. These protections are part of Prisma Cloud's comprehensive approach to securing web applications and APIs against common and severe vulnerabilities.

https://www.paloaltonetworks.com/content/dam/pan/en_US/images/prisma/owasp-top-10- protection-2.png?imwidth=3840 OWASP Top-10 Coverage - Protection against most critical security risks to web applications, including injection flaws, broken authentication, broken access control, security misconfigurations, etc.

Question: 173

Which of the following is displayed in the asset inventory?

A. EC2 instances

B. Asset tags

C. SSO users

D. Federated users

Answer: A

Explanation:

The asset inventory in cloud security platforms like Prisma Cloud typically displays a wide range of cloud resources, including EC2 instances. EC2 instances are virtual servers in Amazon's Elastic Compute Cloud (EC2) for running applications on the Amazon Web Services (AWS) infrastructure. The asset inventory provides visibility into these instances, allowing security teams to monitor their configuration, security posture, and compliance status. This visibility is crucial for identifying misconfigurations, vulnerabilities, and ensuring that all EC2 instances adhere to the organization's security policies and compliance requirements.

https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/prisma-cloud- dashboards/asset-inventory

Question: 174

What is the frequency to create a compliance report? (Choose two.)

A. Weekly

B. One time

C. Monthly

D. Recurring

Answer: B,D

Explanation:

In Prisma Cloud, compliance reports can be generated on a one-time basis or on a recurring schedule. The option for a one-time report allows users to generate a specific report instantly based on the current state of the environment. The recurring option enables users to set up automatic generation of reports at regular intervals, such as weekly or monthly, to track compliance over time. This functionality ensures continuous compliance monitoring and helps in maintaining security standards across cloud resources.

Question: 175

When configuring SSO how many IdP providers can be enabled for all the cloud accounts monitored by Prisma Cloud?

A. 2

B. 4

C. 1

D. 3

Answer: C

Explanation:

Prisma Cloud supports configuring Single Sign-On (SSO) with Identity Providers (IdPs) to streamline user authentication processes. However, for all the cloud accounts monitored by Prisma Cloud, only one IdP provider can be enabled at any

given time. This limitation ensures a unified authentication

mechanism across the platform, reducing complexity and potential security risks associated with managing multiple IdP configurations.

Question: 176

Which two services require external notifications to be enabled for policy violations in the Prisma Cloud environment? (Choose two.)

A. Splunk

B. QROC

C. SQS

D. Email

Answer: A,C

Explanation:

https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/configure-external- integrations-on-prisma-cloud#id24911ff9-c9ec-4503-bb3a-6cfce792a70d

Question: 177

While writing a custom RQL with array objects in the investigate page, which type of auto-suggestion a user can leverage?

A. Auto-sugestion for array objects that are useful for comparing between arrays

B. Auto-suggestion is not available for array objects

C. Auto-suggestion for array objects that are useful for categorization of resource parameters

D. Auto-suggestion for array objects that are useful for comparing between array elements

Answer: B

Explanation:

The auto suggest works with the operators = and IN . It is not supported for array objects. Use

cloud.type attribute to refine the search results. https://docs.paloaltonetworks.com/prisma/prisma- cloud/prisma-cloud-rql-reference/rql-reference/event-query/event-query-attributes

Question: 178

Which file extension type is supported for Malware scanning in Prisma Cloud Data Security (PCDS)?

A. .bat

B. .apk

C. .vb

D. .py

Answer: B

Explanation:

bat --> Data Classification

apk --> Malware Scanning

vb --> Data Classification

py --> Data Classification

https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/prisma-cloud-data- security/monitor-data-security-scan-prisma-cloud/supported-file-extensions

Prisma Cloud Data Security (PCDS) supports various file types for malware scanning, including .apk files, which are Android Package files used for installing applications on Android operating systems. This support is crucial for ensuring that applications deployed on or distributed through Android devices are free from malware and safe for user installation.

Question: 179

Which two bot categories belong to unknown bots under Web-Application and API Security (WAAS) bot protection?

A. News bots

B. Search engine crawlers

C. Web scrapers

D. HTTP libraries

Answer: C,D

Explanation:

Under Web-Application and API Security (WAAS) bot protection in Prisma Cloud, unknown bots are categorized based on their behavior and characteristics. Web scrapers and HTTP libraries fall into the category of unknown bots. Web scrapers are automated scripts or programs that extract data from websites, often without permission, while HTTP libraries are tools used for making HTTP requests. Both can be used benignly but may also be employed in malicious activities, hence their classification as unknown bots requiring further analysis.

Question: 180

In WAAS Access control file upload controls, which three file types are supported out of the box? (Choose three.)

A. Text

B. Images

C. Audio

D. Documents

E. Journal

Answer: A,B,D

Explanation:

In WAAS Access control for file uploads, Prisma Cloud supports various file types out-of-the-box to ensure secure and controlled file upload functionality. The supported file types include Text, Images, and Documents. These categories cover a wide range of commonly used file formats, allowing

organizations to manage and restrict file uploads based on the content type. This feature helps in preventing malicious

file uploads and ensures that only approved file types are uploaded to applications and services.

Question: 181

What are two built-in RBAC permission groups for Prisma Cloud? (Choose two.)

A. Group Membership Admin

B. Group Admin

C. Account Group Admin

D. Account Group Read Only

Answer: A,C

Explanation:

Prisma Cloud includes built-in Role-Based Access Control (RBAC) permission groups to manage user access and permissions efficiently. Among the options, Group Membership Admin and Account Group Admin are two built-in RBAC permission groups. Group Membership Admins are responsible for managing user memberships within groups, while Account Group Admins have administrative privileges over specific account groups, allowing them to manage resources and policies within those groups. These roles help in delegating administrative tasks and enforcing the principle of least privilege.

Question: 182

Which role does Prisma Cloud play when configuring SSO?

A. JIT

B. Service provider

C. SAML

D. Identity provider issuer

Answer: B

Explanation:

When configuring Single Sign-On (SSO) in Prisma Cloud, the platform acts as the Service Provider (SP). In the SSO process, the Service Provider relies on an Identity Provider (IdP) to authenticate users. Prisma Cloud, as the SP, integrates with an IdP to allow users to log in using their existing credentials managed by the IdP. This setup simplifies the authentication process, enhances security by centralizing user credentials, and provides a seamless user experience.

Question: 183

Which Defender type performs registry scanning?

A. Serverless

B. Container

C. Host

D. RASP

Answer: B

Explanation:

In Prisma Cloud, the Defender type responsible for performing registry scanning is the Container Defender. Registry scanning is crucial for ensuring that container images stored in registries are free from vulnerabilities and compliance issues before they are deployed. Container Defenders scan images within container registries, identifying security risks and ensuring that only secure container images are used in deployment, thereby maintaining the integrity and security of containerized applications.

Question: 184

The exclamation mark on the resource explorer page would represent?

A. resource has been deleted

B. the resource was modified recently

C. resource has alerts

D. resource has compliance violation

Answer: C

Explanation:

https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/investigate-incidents- on-prisma-cloud/investigate-config-incidents-on-prisma-cloud

Question: 185

Where are Top Critical CVEs for deployed images found?

A. Defend → Vulnerabilities → Code Repositories

B. Defend → Vulnerabilities → Images

C. Monitor → Vulnerabilities → Vulnerabilities Explorer

D. Monitor → Vulnerabilities → Images

Answer: C

Explanation:

https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/vulnerability_management/vuln_explorer

The top critical CVEs (Common Vulnerabilities and Exposures) for deployed images in Prisma Cloud can be found in the Vulnerabilities Explorer under the Monitor tab. This is where users can input the CVE of interest and get a filtered list of images impacted by that CVE. The Vulnerability Explorer provides a comprehensive view of the vulnerabilities, allowing users to see details such as risk score, CVE risk factors, environmental risk factors, and impacted packages1. This tool is essential for identifying and managing vulnerabilities within your cloud environment, ensuring that all images pulled into deployments or test environments are properly identified and secured.

https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA14u0000004MfoCAE

Question: 186

Which categories does the Adoption Advisor use to measure adoption progress for Cloud Security Posture Management?

A. Visibility, Compliance, Governance, and Threat Detection and Response

B. Network, Anomaly, and Audit Event

C. Visibility, Security, and Compliance

D. Foundations, Advanced, and Optimize

Answer: A

Explanation:

The Adoption Advisor uses four categories to measure adoption progress for Cloud Security Posture Management: Visibility, Compliance, Governance, and Threat Detection and Response. Visibility helps to identify the resources in the environment and to ensure that security controls are in place. Compliance helps to ensure that the environment is meeting regulatory and industry standards. Governance helps to ensure that the environment is secure and managed according to policy. Threat Detection and Response helps to detect and respond to threats quickly and effectively.

The Adoption Advisor in Prisma Cloud uses categories such as Visibility, Compliance, Governance, and Threat Detection and Response to measure adoption progress for Cloud Security Posture Management (CSPM). These categories represent key areas of focus for effectively managing and securing cloud environments. Visibility refers to the ability to see and understand all cloud resources and their configurations. Compliance involves ensuring that cloud resources comply with regulatory standards and best practices. Governance encompasses the policies and procedures that control cloud resource usage and security. Threat Detection and Response involves identifying and mitigating security threats to the cloud environment. By measuring adoption progress across these categories, organizations can assess how well they are utilizing CSPM capabilities to secure their cloud environments.

Question: 187

What are the three states of the Container Runtime Model? (Choose three.)

A. Initiating

B. Learning

C. Active

D. Running

E. Archived

Answer: B,C,E

Explanation:

The Container Runtime Model in Prisma Cloud typically includes states such as Learning, Active, and Archived. The Learning state is where Prisma Cloud observes container behaviors to understand normal operations and establish a baseline. During this phase, the system is not actively enforcing security policies but is learning the typical behaviors and patterns of container activity. The Active state is where the system actively enforces security policies based on the learned behaviors and detected anomalies. Containers that exhibit suspicious or malicious activity that deviates from the baseline may trigger alerts or actions based on configured policies. The Archived state refers to containers that are no longer active but whose data and activity logs are retained for historical analysis or compliance purposes.

Question: 188

What must be created in order to receive notifications about alerts generated when the operator is away from the Prisma Cloud Console?

A. Alarm rule

B. Notification rule

C. Alert rule

D. Ofline alert

Answer: C

Explanation:

https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/manage-prisma- cloud-alerts/prisma-cloud-alert-notifications

Question: 189

Which alerts are fixed by enablement of automated remediation?

A. All applicable open alerts regardless of when they were generated, with alert status updated to "resolved"

B. Only the open alerts that were generated before the enablement of remediation, with alert status updated to "resolved"

C. All applicable open alerts regardless of when they were generated, with alert status updated to "dismissed"

D. Only the open alerts that were generated after the enablement of remediation, with alert status updated to "resolved"

Answer: A

Explanation:

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.

Question: 190

Which two statements apply to the Defender type Container Defender - Linux?

A. It is implemented as runtime protection in the userspace.

B. It is deployed as a service.

C. It is deployed as a container.

D. It is incapable of filesystem runtime defense.

Answer: A,C

Explanation:

The Defender type "Container Defender - Linux" in Prisma Cloud is typically deployed as a container. This deployment method allows the Defender to integrate seamlessly into containerized environments, providing runtime protection and monitoring for container activities. By running as a container, the Container Defender can leverage the native capabilities of the container orchestration platform, such as Kubernetes, to provide security features like threat detection,

vulnerability management, and compliance enforcement within the containerized environment. This approach ensures that the security protections are closely aligned with the dynamic and scalable nature of containerized applications.

Question: 191

Which field is required during the creation of a custom config query?

A. resource status

B. api.name

C. finding.type

D. cloud.type

Answer: B

Explanation:

During the creation of a custom config query in Prisma Cloud, the "api.name" field is required. This field specifies the API endpoint that the query will target, essentially defining the scope of the query within the cloud environment. The "api.name" serves as a critical identifier that allows the query to retrieve specific information or perform actions related to the chosen API endpoint. By specifying the "api.name," users can create tailored queries that address their specific security, compliance, or governance needs, enabling more precise and effective management of cloud resources and security posture.

Question: 192

Which role must be assigned to DevOps users who need access to deploy Container and Host Defenders in Compute?

A. Cloud Provisioning Admin

B. Build and Deploy Security

C. System Admin

D. Developer

Answer: A

Explanation:

Cloud Provisioning Admin (Defender Manager) DevOps team members that need to manage Defender deployments without sysadmin privileges.
https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/authentication/prisma_cloud_user_roles

Question: 193

Which three serverless runtimes are supported by Prisma Cloud for vulnerability and compliance scans? (Choose three.)

A. Swift

B. Python

C. Dart

D. Java

E. Node.js

Answer: B,D,E

Explanation:

Prisma Cloud supports several serverless runtimes for vulnerability and compliance scans, including Python, Java, and Node.js. These runtimes are widely used in the development of serverless applications, which are designed to run in stateless compute containers that are event-triggered and fully managed by cloud services. By providing vulnerability and compliance scans for these serverless runtimes, Prisma Cloud helps organizations identify and remediate security issues within their

serverless applications, ensuring that they adhere to security best practices and compliance standards. This capability is crucial for maintaining the security and integrity of serverless architectures, where traditional security approaches may not be applicable.

Question: 194

Which two attributes are required for a custom config RQL? (Choose two.)

A. json.rule

B. cloud.account

C. api.name

D. tag

Answer: A,C

Explanation:

For a custom config Resource Query Language (RQL) in Prisma Cloud, two essential attributes are "json.rule" and "api.name." The "json.rule" attribute allows users to specify the JSON structure that defines the criteria or conditions of the query, essentially dictating what the query is looking for within the cloud environment. The "api.name" attribute identifies the specific API endpoint that the query will target, providing context and scope for the query. Together, these attributes enable users to craft precise and targeted queries that can assess the configuration and security posture of cloud resources, aiding in compliance checks, security assessments, and other governance tasks.

Question: 195

Which type of query is used for scanning Infrastructure as Code (IaC) templates?

A. API

B. XML

C. JSON

D. RQL

Answer: C

Explanation:

https://www.paloaltonetworks.com/blog/prisma-cloud/cloud-iac-build-policies/

Question: 196

A Prisma Cloud Administrator onboarded an AWS cloud account with agentless scanning enabled successfully to Prisma Cloud. Which item requires deploying defenders to be able to inspect the risk on the onboarded AWS account?

A. Host compliances risks

B. Container runtime risks

C. Container vulnerability risks

D. Host vulnerability risks

Answer: B

Explanation:

While agentless scanning in Prisma Cloud can effectively assess various risks in cloud environments, including host compliance and vulnerabilities, it does not extend to container runtime risks. To inspect risks associated with container runtimes, such as real-time threat detection, behavioral monitoring, and deep visibility into container activity, deploying Prisma Cloud Defenders is necessary. These Defenders are lightweight agents that provide an additional layer of security by monitoring containerized applications in real-time, thereby offering comprehensive protection against threats that may arise during the runtime phase of containers.

Question: 197

What are the subtypes of configuration policies in Prisma Cloud?

A. Build and Deploy

B. Monitor and Analyze

C. Security and Compliance

D. Build and Run

Answer: D

Explanation:

In Prisma Cloud, configuration policies are categorized to align with the different phases of the cloud security lifecycle, emphasizing a holistic approach to cloud security management. The subtypes "Build and Run" encapsulate this approach by covering both the development phase (Build) - where cloud resources and applications are designed and created, and the operational phase (Run) - where these resources and applications are deployed and actively used. This categorization ensures that security and compliance are integral throughout the lifecycle, from the initial creation of cloud infrastructure and applications to their deployment and day-to-day operation, thereby enhancing the overall security posture.

Question: 198

Which Prisma Cloud policy type can protect against malware?

A. Event

B. Network

C. Config

D. Data

Answer: D

Explanation:

The "Data" policy type in Prisma Cloud is specifically designed to protect against threats related to data, including malware. These policies focus on securing data at rest and in transit, implementing data loss prevention (DLP) mechanisms, and scanning data stores and payloads for malicious content. By employing data policies, Prisma Cloud ensures that data stored within cloud environments is safeguarded against unauthorized access, exfiltration, and malware, thereby maintaining the integrity and confidentiality of sensitive information.

Question: 199

Which of the following is not a supported external integration for receiving Prisma Cloud Code

Security notifications?

A. Splunk

B. Cortex XSOAR

C. Microsoft Teams

D. ServiceNow

Answer: D

Explanation:

Prisma Cloud enables you to send notifications for new code and CI/CD security issues detected during periodic scans of your environments to messaging systems that you have integrated with Prisma Cloud. Supported messaging systems include Microsoft Teams, Slack, Splunk, JIRA, ServiceNow notification systems, as well as for webhooks.

https://docs.prismacloud.io/en/classic/appsec-admin-guide/get-started/finetune-configuration- settings/enable-notifications

Question: 200

How is the scope of each rule determined in the Prisma Cloud Compute host runtime policy?

A. By the collection assigned to that rule

B. By the target workload

C. By the order in which it is created

D. By the type of network traffic it controls

Answer: A

Explanation:

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.

Question: 201

A Prisma Cloud Administrator needs to enable a Registry Scanning for a registry that stores Windows images. Which of the following statement is correct regarding this process?

A. They can deploy any type of container defender to scan this registry.

B. There are Windows host defenders deployed in your environment already.

C. There are Windows host defenders deployed in your environment already. Therefore, they do not need to deploy any additional defenders.

D. A defender is not required to configure this type of registry scan.

Answer: B

Explanation:

When enabling Registry Scanning in Prisma Cloud for a registry that stores Windows images, it's important to note that Windows host defenders must be deployed in the environment to scan these images effectively. The Windows host defenders are specialized versions of the Prisma Cloud Defender that are designed to run on Windows operating systems. They provide the necessary functionality to scan Windows container images stored in registries, identifying vulnerabilities and ensuring the images comply with security policies before they are deployed. This requirement underscores the importance of having the appropriate Defender deployments that match the operating systems of the images being scanned.

Question: 202

Prisma Cloud Compute has been installed on Onebox. After Prisma Cloud Console has been accessed. Defender is disconnected and keeps returning the error "No console connectivity" in the logs.

What could be causing the disconnection between Console and Defender in this scenario?

A. Port 8083 is not open for Console and Defender communication.

B. The license key provided to the Console is invalid.

C. Port 8084 is not open for Console and Defender communication.

D. Onebox script installed an older version of the Defender.

Answer: C

Explanation:

By default, Defender is configured to communicate with Console on port 8084. If port 8084 is closed, then Defender cannot communicate with Console.

https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000PNWXCA4#:~:text=If%20port%208084%20is%20closed%2C%20then%20Defender%20cannot%20communicate%20with%20Console.&text=Resolve%20the%20issue%20by%20setting,%3E%20Load%20Balancer%20%3E%20Defender).

Question: 203

Which resources can be added in scope while creating a vulnerability policy for continuous integration?

A. Labels and AccountID

B. Images and labels

C. Images and cluster

D. Images and containers

Answer: D

Explanation:

When creating a vulnerability policy for continuous integration within Prisma Cloud, the scope of the policy can include specific resources that are critical to the CI/CD pipeline, such as images and containers. These resources are central to the development and deployment processes in containerized environments. By focusing on images and containers, the policy can effectively identify and address vulnerabilities that might be present in container images before they are deployed or in running containers, thereby enhancing the security of the continuous integration and deployment pipeline. This approach ensures that only secure, compliant container images are used in production,

reducing the risk of vulnerabilities being exploited.

Question: 204

Which statement applies to Adoption Advisor?

A. It helps adopt security capabilities at a fixed pace regardless of the organization's needs.

B. It only provides guidance during the deploy phase of the application lifecycle.

C. It is only available for organizations that have completed the cloud adoption journey.

D. It includes security capabilities from subscriptions for CSPM, CWP, CCS, OEM, and Data Security.

Answer: D

Explanation:

Adoption Advisor is a feature within Prisma Cloud that provides organizations with guidance on adopting various security capabilities based on their unique needs and the stage they are at in their cloud security journey. It doesn't enforce a fixed pace but rather suggests a tailored path for enhancing security posture, taking into account the organization's specific requirements and the complexity of their cloud environment. The Adoption Advisor supports a broad range of security capabilities, encompassing Cloud Security Posture Management (CSPM), Cloud Workload Protection (CWP), Cloud Code Security (CCS), Out-of-Band (OEM), and Data Security. This comprehensive approach ensures that organizations can secure their cloud environments effectively across different phases of the application lifecycle, from development to deployment, and across various cloud resources and services.

Question: 205

Which type of RQL query should be run to determine if AWS Elastic Compute Cloud (EC2) instances without encryption was enabled?

A. NETWORK

B. EVENT

C. CONFIG

D. SECURITY

Answer: C

Explanation:

To determine if AWS EC2 instances are running without encryption enabled, the appropriate RQL (Resource Query Language) type to use is CONFIG. CONFIG queries in Prisma Cloud are designed to inspect the configuration states of cloud resources and identify compliance with best practices or specific security requirements. By running a CONFIG query, administrators can assess the configuration settings of EC2 instances, including whether encryption features are enabled or not. This type of query allows for deep inspection of resource configurations within cloud environments,

making it the ideal choice for identifying unencrypted EC2 instances and thereby helping to ensure data protection and compliance with security policies.

Question: 206

How does assigning an account group to an administrative user on Prisma Cloud help restrict access to resources?

A. It restricts access only to certain types of resources within the cloud account.

B. It restricts access to all resources and data within the cloud account.

C. It restricts access only to the resources and data that pertains to the cloud account(s) within an account group.

D. It does not restrict access to any resources within the cloud account.

Answer: C

Explanation:

In Prisma Cloud, assigning an administrative user to an account group is a way to implement the principle of least privilege by restricting the user's access to a specific subset of resources and data. Account groups are logical collections of cloud accounts, and by associating an administrative user with a particular account group, their access is limited to only those resources and data associated with the cloud accounts within that group. This mechanism ensures that users have access only to the information and resources necessary for their role or tasks, enhancing security by minimizing the potential for unauthorized access or actions within the cloud environment.

Question: 207

Which RQL query will help create a custom identity and access management (1AM) policy to alert on Lambda functions that have permission to terminate EC2 instances?

A. iam from cloud.resource where dest.cloud.type = 'AWS' AND source.cloud.service.name = 'lambda' AND source.cloud.resource.type = 'function' AND dest.cloud.service.name = 'ec2' AND action.name = 'ec2:TerminateInstances'

B. config from iam where dest.cloud.type = 'AWS' AND source.cloud.service.name = 'ec2' AND source.cloud.resource.type = 'instance' AND dest.cloud.service.name = 'lambda' AND action.name = 'ec2:TerminateInstances'

C. iam from cloud.resource where cloud.type equals 'AWS' AND cloud.resource.type equals 'lambda function' AND cloud.service.name = 'ec2' AND action.name equals 'ec2:TerminateInstances'

D. config from iam where dest.cloud.type = 'AWS' AND source.cloud.service.name = 'lambda' AND source.cloud.resource.type = 'function' AND dest.cloud.service.name = 'ec2' AND action.name = 'ec2:TerminateInstances'

Answer: D

Explanation:

Question: 208

In which Console menu would an administrator verify whether a custom compliance check is failing or passing?

A. Monitor > Compliance

B. Container Security > Compliance

C. Defend > Compliance

D. Custom > Compliance

Answer: A

Explanation:

In Prisma Cloud, the "Monitor > Compliance" menu is the centralized location where administrators can verify the status of custom compliance checks, along with predefined compliance standards and frameworks. This section provides a comprehensive view of the organization's compliance posture, displaying whether specific compliance checks are passing or failing. It allows for detailed insights

into compliance status across cloud environments, helping administrators identify areas of noncompliance, understand the reasons behind compliance failures, and take corrective actions to address any identified issues.

Question: 209

Which two frequency options are available to create a compliance report within the console? (Choose two.)

A. One-time

B. Monthly

C. Recurring

D. Weekly

Answer: A,D

Explanation:

Within Prisma Cloud, when creating compliance reports, administrators have the flexibility to schedule the generation of these reports based on their specific needs. The available frequency options include "One-time," where a report is generated once at a specified time, and "Weekly," which allows for the recurring generation of reports on a weekly basis. These options provide organizations with the ability to tailor their compliance reporting to their operational requirements, ensuring that they have regular and up-to-date insights into their compliance posture.

Question: 210

Which Prisma Cloud policy type detects port scanning activities in a customer environment?

A. Port Scan

B. Anomaly

C. Config

D. Network

Answer: B

Explanation:

In the context of Prisma Cloud, the policy type that is specifically designed to detect unusual activities, such as port scanning, within a customer's environment is classified under "Anomaly." Anomaly-based policies leverage advanced analytics and machine learning algorithms to identify patterns and behaviors that deviate from the norm, which could indicate potential security threats like port scanning attempts. By detecting such anomalies, these policies help organizations proactively identify and respond to potential reconnaissance activities by attackers seeking to discover open ports and vulnerable services.

Question: 211

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.

Question: 212

Which command should be used in the Prisma Cloud twistcli tool to scan the nginx:latest image for vulnerabilities and compliance issues?

A)

B)

```
$ twistcli images scan
"address <COMPUTE_CONSOLE>
— i^rname <COMPUTE_CONSOLE_USER>
—password <COMPmj^NSOLE_PASSWD>
--details
nginx:latest
```

C)

```
$ twistcli images scan
—address <COMPUTE_CON5GLE>
—user <C®MPUTE.J^S^^
—password <COMPUTE_CONSOLE^PASSWD>
—details
nginx:latest
```

D)

A. Option A

B. Option B

C. Option C

D. Option D

Answer: D

Explanation:

The correct command to scan the nginx:latest image for vulnerabilities and compliance issues using the Prisma Cloud twistcli tool is shown in Option D. This command uses twistcli images scan with specified parameters for the console address, username, and password, and it outputs the results to a file named scan-results.json. This allows for the

scanning results to be saved and reviewed in a structured format, which aids in further analysis and tracking of vulnerabilities and compliance issues.

Question: 213

Based on the following information, which RQL query will satisfy the requirement to identify VM hosts deployed to organization public cloud environments exposed to network traffic from the internet and affected by Text4Shell RCE (CVE-2022-42889) vulnerability?

- Network flow logs from all virtual private cloud (VPC) subnets are ingested to the Prisma Cloud Enterprise Edition tenant.
- All virtual machines (VMs) have Prisma Cloud Defender deployed.

A)

B)

C)

D)

A. Option A
B. Option B
C. Option C
D. Option D

Answer: A

Explanation:

The RQL query in Option A is designed to identify VM hosts that are exposed to internet traffic and are affected by the Text4Shell RCE vulnerability (CVE-2022-42889). This query looks for network flow records with byte transfers indicating activity and filters for resources with host vulnerability findings sourced from 'Prisma Cloud'. It also checks for exposure to suspicious or internet IPs, satisfying the criteria for the given scenario.

www.atmicnetworks.com

Question: 214

What is the purpose of Incident Explorer in Prisma Cloud Compute under the "Monitor" section?

A. To sort through large amounts of audit data manually in order to identify developing attacks

B. To store large amounts of forensic data on the host where Console runs to enable a more rapid and effectiveresponse to incidents

C. To correlate individual events to identify potential attacks and provide a sequence of process, file system, and network events for a comprehensive view of an incident

D. To identify and suppress all audit events generated by the defender

Answer: C

Explanation:

The purpose of Incident Explorer in Prisma Cloud Compute under the "Monitor" section is to provide a comprehensive view of incidents by correlating individual events. This helps identify potential attacks through a sequence of processes, file system, and network events, thereby giving a complete picture of an incident's timeline and impact.

https://docs.prismacloud.io/en/classic/compute-admin-guide/runtime-defense/incident-explorer

Question: 215

Which RQL will trigger the following audit event activity?

A. event from cloud.audit_logs where operation ConsoleLogin AND user = 'root'

B. event from cloud.audit_logs where operation IN('cloudsql.instances.update','cloudsql.sslCerts.create', cloudsql.instances.create','cloudsq

C. event from cloud.audit_logs where cloud.service = s3.amazonaws.com' AND json.rule = $.userAgent contains 'parrot1

D. event from cloud.audit_logs where operation IN ('GetBucketWebsite', 'PutBucketWebsite', 'DeleteBucketWebsite')

Answer: A

Explanation:

The correct RQL to trigger the audit event activity shown is Option A. This RQL is designed to capture events from cloud audit logs where a ConsoleLogin operation occurs by the 'root' user. The given audit event details match this RQL's criteria, which specifies the operation type and the user involved in the event.

Question: 216

Prisma Cloud cannot integrate which of the following secrets managers?

A. IBM Secret Manager

B. AzureKey Vault

C. HashiCorp Vault

D. AWS Secret Manager

Answer: A

Explanation:

Prisma Cloud integrates with various secret managers to manage sensitive information such as passwords, tokens, and keys. However, it cannot integrate with IBM Secret Manager. The other options, Azure Key Vault, HashiCorp Vault, and AWS Secret Manager, are supported for integration with Prisma Cloud, providing secure storage and handling of secrets.

Question: 217

DRAG DROP

Put the steps of integrating Okta with Prisma Cloud in the right order in relation to CIEM or SSO okra integration.

Log in to your Okta administrator panel.

Add an administrator role.

Generate an API token

Configure Okta with Prisma Cloud

Run the 1AM queries for Okta

Answer Area j

Answer:

Explanation:

Log in to your Okta administrator panel.

Add an administrator role.

Generate an API token.

Configure Okta with Prisma Cloud.

Run the IAM queries for Okta.

When integrating Okta with Prisma Cloud, especially in the context of Cloud Infrastructure Entitlement Management (CIEM) or Single Sign-On (SSO) integration, the process must be conducted in a sequence that establishes the necessary permissions and configurations for successful integration.

The first step is to log in to the Okta administrator panel. This is where you will manage your Okta settings and begin the integration process.

Once logged in, the next step is to add an administrator role. This involves assigning a role within Okta that has the appropriate permissions to create and manage API tokens and to perform integration tasks.

After setting up the correct administrative role, the third step is to generate an API token. This token will be used to authenticate the communications between Okta and Prisma Cloud. The API token acts as a secure method of verifying that requests made to Prisma Cloud are authorized.

www.atmicnetworks.com

With the API token generated, the fourth step is to configure Okta with Prisma Cloud. This step typically involves entering the API token into Prisma Cloud and setting up the necessary configurations within Prisma Cloud to recognize and accept authentication requests from Okta.

The final step is to run the Identity and Access Management (IAM) queries for Okta within Prisma Cloud. This step is crucial for CIEM, as it allows Prisma Cloud to query Okta for identity information, user roles, and entitlements, ensuring that the correct permissions are enforced across the cloud environment and that SSO is functioning correctly.

Following these steps in order will ensure that Okta is properly integrated with Prisma Cloud, providing a secure and efficient method for managing cloud access and entitlements.

Question: 218

On which cloud service providers can new API release information for Prisma Cloud be received?

A. AWS. Azure. GCP. Oracle, IBM

B. AWS. Azure. GCP, IBM, Alibaba

C. AWS. Azure. GCP. Oracle, Alibaba

D. AWS. Azure. GCP, IBM

Answer: C

Explanation:

Based on the information available in the provided documents, specifically from the "code-to-cloud-intelligence (1).pdf", Prisma Cloud by Palo Alto Networks offers integration with multiple cloud service providers. While the document does not explicitly mention the ability to receive new API release information for Prisma Cloud, it does list integrations with various cloud service providers such as AWS, Azure, Google Cloud (GCP), Oracle Cloud, and Alibaba Cloud. Therefore, the answer would be C: AWS, Azure, GCP, Oracle, Alibaba.

Question: 219

Which command correctly outputs scan results to stdout in tabular format and writes scan results to

a JSON file while still sending the results to Console?

A. $ twistcli images scan--address--user--password--stdout-tabular--output-file scan-results.jsonnginx:latest

B. $ twistcli images scan--address--username--password--details--json-output scan-results.jsonnginx:latest

C. $ twistcli images scan--address--user--password--details--file-output scan-results.jsonnginx:latest

D. $ twistcli images scan--address--u--p--details--output-file scan-results.jsonnginx:latest

Answer: C

Explanation:

The correct command to output scan results to stdout in tabular format and write scan results to a JSON file while still sending the results to Console is:

$ twistcli images scan \

--address <console_address> \

--user <username> \

--password <password> \

--output-file scan-results.json \

--publish \

nginx:latest

This command uses the --output-file option to write the scan results to a file and the --publish option to send the results to the Console. The --stdout-tabular option is not necessary as by default, twistcli writes scan results to stdout in a human-readable format. The placeholders <console_address>, <username>, and <password> should be replaced with the actual address of the Console, and the user's credentials12.

Please replace the placeholders with your actual Prisma Cloud Console address and credentials to execute the command successfully. If you have any more questions or need further assistance, feel free to ask.

Question: 220

Which two proper agentless scanning modes are supported with Prisma Cloud? (Choose two).

A. Spoke Account Mode

B. Hub Account Mode

C. Same Account Mode

D. Main Account Mode

Answer: A,B

Explanation:

Prisma Cloud supports different scanning modes for its agentless scanning feature. Based on the context of cloud environments and typical terminology used in Prisma Cloud documentation, "Spoke Account Mode" and "Hub Account Mode" are plausible modes supported for agentless scanning. These modes allow for the extension of scanning capabilities across multiple accounts, with 'Spoke' typically referring to linked accounts and 'Hub' referring to the central account in a hub-and-spoke architecture. Hence, the correct answers are A and B.

Question: 221

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.

Question: 222

What is required for Prisma Cloud to successfully execute auto-remediation commands?

A. Read access to the cloud platform

B. Write access to the cloud platform

C. Access to the cloud platform only for Azure

D. Prisma Cloud requires no access to the cloud platform

Answer: B

Explanation:

For Prisma Cloud to execute auto-remediation commands, it requires write access to the cloud platform. This is because auto-remediation involves making changes to configurations or settings within the cloud environment to rectify security issues. Thus, the correct answer is B: Write access to the cloud platform.

Question: 223

What is a benefit of the Cloud Discovery feature?

A. It does not require any specific permissions to be granted before use.

B. It helps engineers find all cloud-native services being used only on AWS.

C. It offers coverage for serverless functions on AWS only.

D. It enables engineers to continuously monitor all accounts and report on the services that are unprotected.

Answer: D

Explanation:

The Cloud Discovery feature in Prisma Cloud allows engineers to monitor accounts continuously and report on cloud-native services that are unprotected across different cloud service providers. This feature requires specific permissions to access and assess the cloud environment's configuration and security posture. Thus, the correct answer is D: It enables engineers to continuously monitor all accounts and report on the services that are unprotected.

https://docs.prismacloud.io/en/classic/compute-admin-guide/cloud-service-providers/cloud- accounts-

discovery-pcee

Question: 224

In Prisma Cloud for Azure Net Effective Permissions Calculation, the following Azure permission levels are supported by which three permissions? (Choose three).

A. Resources

B. Tenant

C. Subscription

D. Resource groups

E. Management Group

Answer: A,C,E

Explanation:

https://docs.prismacloud.io/en/classic/cspm-admin-guide/prisma-cloud-iam-security/context-used- to-calculate-effective-permissions

Question: 225

Given the following information, which twistcli command should be run if an administrator were to exec into a running container and scan it from within using an access token for authentication?

- Console is located at https://prisma-console.mydomain.local
- Token is: TOKEN_VALUE
- Report ID is: REPORTJD
- Container image running is: myimage:latest

A. twistcli images scan --address https://prisma-console.mydomain.local —token TOKENVALUE — containerized —details myimage:latest

B. twistcli images scan —console-address https://prisma-console.mydomain.local —auth-token MY_TOKEN —local-scan —details myimage:latest

C. twistcli images scan —address https://prisma-console.mydomain.local —token TOKEN_VALUE —

containerized --details REPORT_ID

D. twistcli images scan --console-address https://prisma-console.mydomain.local --auth-token TOKEN_VALUE —containerized —vulnerability-details REPORT_ID

Answer: C

Explanation:

The response from Jihe would be correct if this wasn't be run from within the container. In the question, we are running from inside the container, and therefor there is no need to specify an image/tarball. https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/tools/twistcli_scan_image Further down in the documentation linked by Jihe, there is a section that shows the proper syntax when running twistcli from within a container. The example there is almost a perfect copy of this question. Spippolo has the correct response.

$ docker run \

- v /PATH/TO/TWISTCLI_DIR:/tools \
- e TW_TOKEN=<API_TOKEN> \
- e TW_CONSOLE=<COMPUTE_CONSOLE> \
- -entrypoint="" \
- IMAGE_NAME> \

/tools/twistcli images scan \

- -containerized \
- -details \
- -address $TW_CONSOLE \
- -token $TW_TOKEN \

<REPORT_ID>

https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/tools/twistcli_scan_images

Question: 226

Prisma Cloud supports which three external systems that allow the import of vulnerabilities and provide additional context on risks in the cloud? (Choose three.)

A. Splunk

B. Qualys

C. Amazon Inspector

D. Amazon GuardDuty

E. ServiceNow

Answer: B,C,D

Explanation:

Similarly, Prisma Cloud integration with external systems such as Amazon GuardDuty, AWS Inspector, Qualys, and Tenable allow you to import vulnerabilities and provide additional context on risks in the cloud. https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/configure- external-integrations-on-prisma-cloud

Question: 227

Which policy type should be used to detect and alert on cryptominer network activity?

A. Audit event

B. Anomaly

C. Config-build

D. Config-run

Answer: B

Explanation:

To detect and alert on cryptominer network activity, the policy type that should be used is an Anomaly policy. Anomaly policies in Prisma Cloud are designed to identify unusual and potentially malicious activities, including the network patterns typical of cryptomining operations. These policies leverage behavioral analytics to spot deviations from normal operations, making Option B the correct answer.

Suspicious network actors—Exposes suspicious connections by inspecting the network traffic to and from your cloud environment and correlating it with AutoFocus, Palo Alto Networks threat intelligence feed. AutoFocus identifies IP addresses involved in suspicious or malicious activity and classifies them into one of eighteen categories. Some examples of the categories are Backdoor, Botnet, Cryptominer, DDoS, Ransomware, Rootkit, and Worm. There are thirty-six policies, two for each of the eighteen categories—internal and external.

https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/prisma-cloud-policies/anomaly-policies

Question: 228

Which three AWS policy types and identities are used to calculate the net effective permissions? (Choose three).

A. AWS service control policies (SCPs)

B. AWS IAM group

C. AWS IAM role

D. AWS IAM User

E. AWS IAM tag policy

Answer: A,B,C

Explanation:

In AWS, the net effective permissions are calculated based on various policy types and identities. The correct choices are:

A . AWS service control policies (SCPs): SCPs are used in AWS Organizations to manage permissions for all accounts within the organization, affecting the net effective permissions.

B . AWS IAM group: IAM groups define a set of permissions for a collection of users, influencing their effective permissions.

C . AWS IAM role: IAM roles provide temporary security credentials to assume a set of permissions, impacting the net effective permissions. Option D (AWS IAM User) and E (AWS IAM tag policy) also play roles in defining permissions, but A, B, and C are the primary types used in calculating net effective permissions, making them the correct choices.

Question: 229

Which three platforms support the twistcli tool? (Choose three.)

A. Linux

B. Windows

C. Android

D. MacOS

E. Solaris

Answer: A,B,D

Explanation:

The twistcli tool, part of Prisma Cloud's suite of security tools, supports various platforms for security scanning and configuration. The correct platforms supported by twistcli include:

A . Linux: twistcli is widely used on Linux platforms for scanning container images, host vulnerabilities, and more, making it a correct choice.

B . Windows: twistcli supports Windows, allowing users to perform security scans and checks on Windows-based systems, making it a correct choice.

D . MacOS: twistcli is also compatible with MacOS, enabling security operations on Apple's operating system, making it a correct choice. Option C (Android) and E (Solaris) are not supported platforms for the twistcli tool, according to the available documentation on Prisma Cloud.

Question: 230

Which policy type provides information about connections from suspicious IPs in a customer database?

A. Anomaly

B. Threat detection

C. Network

D. AutoFocus

Answer: A

Explanation:

https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/prisma-cloud-policies/anomaly-policies

An Anomaly policy in Prisma Cloud is designed to provide information about connections from suspicious IPs in a customer database. Anomaly policies are used to detect and alert on unusual activities that deviate from the norm, which can include traffic from known malicious or suspicious IP addresses. These policies help in identifying potential security threats by monitoring for activities that are out of the ordinary, such as unexpected access to a database from an IP address that has not been seen before or is known to be associated with malicious activities.

The documentation link you provided offers detailed guidance on how to configure and manage anomaly policies in Prisma Cloud, ensuring that users can effectively monitor their environments for potential security incidents.

Question: 231

A customer wants to monitor its Amazon Web Services (AWS) accounts via Prisma Cloud, but only needs the resource configuration to be monitored at present.

Which two pieces of information are needed to onboard this account? (Choose two.)

A. External ID

B. CloudTrail

C. Active Directory ID

D. RoleARN

Answer: A,D

Explanation:

To onboard an AWS account for monitoring by Prisma Cloud, specifically for resource configuration monitoring, the required pieces of information include:

A . External ID: The External ID is a unique identifier used in the trust relationship between Prisma Cloud and the AWS account, ensuring secure access, making it a correct choice.

D . RoleARN: The Role Amazon Resource Name (RoleARN) is necessary to grant Prisma Cloud the required permissions to access and monitor the AWS account resources, making it a correct choice. Option B (CloudTrail) is related to AWS logging but is not required solely for onboarding. Option C (Active Directory ID) is not relevant to AWS account onboarding for Prisma Cloud.

Question: 232

A container and image compliance rule has been configured by enabling all checks; however, upon review, the container's compliance view reveals only the entries in the image below.

What is the appropriate action to take next?

A. Deploy defenders to scan complete container compliance.

B. Wait until Prisma Cloud finishes the compliance scan and recheck.

C. Change the rule options to list both failed and passed checks in the compliance rule edit window.

D. Change the rule options to list only failed checks in the compliance rule edit window.

Answer: C

Explanation:

The image provided showcases a filtered compliance view, which is displaying only certain checks with varying severities and descriptions related to container and image compliance. Since the compliance rule was configured to enable all checks but only a subset of entries is visible, it implies that the current view is filtered to show specific entries. To obtain a comprehensive view of all checks, including those that have passed, the rule options must be adjusted. By selecting the option to list both failed and passed checks, one can gain complete visibility over the compliance status of the container, ensuring that no aspect of the compliance has been overlooked and that all necessary information is available for review.

Question: 233

What is the primary purpose of Prisma Cloud Code Security?

A. To provide a platform for developers to create custom security policies for applications

B. To triage alerts and incidents in realtime during deployment

C. To address cloud infrastructure misconfigurations in code before they become alerts or incidents

D. To offer instant feedback on application performance issues and bottlenecks

Answer: C

Explanation:

Prisma Cloud Code Security is designed to integrate security into the DevOps process by scanning infrastructure as code (IaC) templates and configurations for potential security issues. This proactive approach allows developers and security teams to address misconfigurations and vulnerabilities in the code itself, before they are deployed into the cloud environment and become more challenging to resolve. By identifying and rectifying these issues early in the development lifecycle, organizations can reduce the risk of alerts and incidents arising from misconfigurations in their cloud infrastructure, leading to a more secure and compliant cloud environment.

Question: 234

A Systems Engineer is the administrator of a self-hosted Prisma Cloud console. They upgraded the console to the latest version. However, after the upgrade, the console does not show all the policies configured. Before they upgraded the console, they created a backup manually and exported it to a local drive. Now they have to install a Prisma Cloud to restore from the backup that they manually created. Which Prisma Cloud version can they can restore with the backup?

A. Any version of Prisma Cloud Self-Hosted Console

B. Up to N-2 versions of the Prisma Cloud Self-Hosted Console that the backup created

C. The same version of the Prisma Cloud Self-Hosted Console that the backup created

D. The latest version of Prisma Cloud Self-Hosted Console

Answer: C

Explanation:

https://docs.prismacloud.io/en/compute-edition/31/admin-guide/configure/disaster-recovery

In scenarios where a backup is created manually before upgrading a self-hosted console, it is crucial to restore the system using the backup that matches the version of the Prisma Cloud Self-Hosted Console from which it was taken. This ensures compatibility and integrity of the data and configurations. Using a backup with a different version of the console may lead to inconsistencies or loss of information due to potential changes in the software's data structures or features between versions. Therefore, to ensure a successful restoration, the backup must be applied to the same version of the Prisma Cloud Self-Hosted Console that it was created from.

Question: 235

Which ROL query is used to detect certain high-risk activities executed by a root user in AWS?

A. event from cloud.audit_logs where operation IN ('ChangePassword', 'ConsoleLogin', 'DeactivateMFADevice', 'DeleteAccessKey' , 'DeleteAlarms') AND user = 'root'

B. event from cloud.security_logs where operation IN ('ChangePassword', 'ConsoleLogin', 'DeactivateMFADevice', 'DeleteAccessKey' , 'DeleteAlarms') AND user = 'root'

C. config from cloud.audit_logs where operation IN ('ChangePassword', 'ConsoleLogin', 'DeactivateMFADevice', 'DeleteAccessKey', 'DeleteAlarms') AND user = 'root'

D. event from cloud.audit_logs where Risk.Level = 'high' AND user = 'root'

Answer: A

Explanation:

https://docs.prismacloud.io/en/classic/rql-reference/rql-reference/event-query/event-query-examples https://docs.prismacloud.io/en/classic/rql-reference/rql-reference/event-query/event-query-examples#idda895fd2-4496-4b31-9766-7d50215dcc18

Question: 236

Which two information types cannot be seen in the data security dashboard? (Choose two).

A. Bucket owner

B. Object Data Profile by Region

C. Top Publicly Exposed Objects By Data Profile

D. Object content

E. Total objects

Answer: A,D

Explanation:

The data security dashboard in Prisma Cloud provides a comprehensive overview of the security posture related to cloud data storage. However, certain information types, such as the identity of the bucket owner and the actual content within an object, are not typically displayed on such dashboards. This is because the dashboard focuses more on aggregated data profiles, exposure levels, and compliance-related information rather than individual ownership details or the specific content of objects, which may require separate detailed analysis or are managed through different security mechanisms.

Question: 237

Taking which action will automatically enable all severity levels?

A. Navigate to Settings > Enterprise Settings and enable all severity levels in the alarm center.

B. Navigate to Policies > Settings and enable all severity levels in the alarm center.

C. Navigate to Settings > Enterprise Settings and ensure all severity levels are checked under "auto-enable default policies.

D. Navigate to Policies > Settings and ensure all severity levels are checked under "auto-enable default policies.

Answer: D

Explanation:

In Prisma Cloud, to automatically enable all severity levels for alerts, a user would need to navigate to the Policies section, then to Settings. Within this area, there is an option for "auto-enable default policies," which, when checked for all severity levels, ensures that any default policies related to those severities are automatically activated. This is a configuration setting that streamlines the alerting process by ensuring that all relevant severity levels are covered by the default policies without the need for manual intervention.

https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/prisma-cloud-policies/manage-prisma-cloud-policies

Step 1- To enable global settings for Prisma Cloud default policies click "Settings" and select "Enterprise Settings" Step 2- To enable policies based on severity, select Auto enable new default policies of the type—Critical, High, Medium, Low or Informational.

Question: 238

Which two elements are included in the audit trail section of the asset detail view? (Choose two).

A. Configuration changes

B. Findings

C. Overview

D. Alert and vulnerability events

Answer: A,D

Explanation:

The audit trail section of an asset's detail view in Prisma Cloud typically includes a log of configuration changes and alert and vulnerability events associated with the asset. These elements are crucial for tracking the history of modifications to an asset's configuration and the security incidents that have affected it. This information is instrumental in understanding the security posture of the asset over time and in conducting thorough investigations after a security event has been detected.

Question: 239

Which step should a SecOps engineer implement in order to create a network exposure policy that identifies instances accessible from any untrusted internet sources?

A. In Policy Section-> Add Policy-> Config type -> Define Policy details Like Name,Severity-> Configure RQL query "config from network where source.network = UNTRUSTJNTERNET and dest.resource.type = 'Instance' and dest.cloud.type = 'AWS*'" -> define compliance standard -> Define recommendation for remediation & save.

B. In Policy Section-> Add Policy-> Network type -> Define Policy details Like Name.Severity-> Configure RQL query "network from vpc.flow_record where source.publicnetwork IN ('Suspicious IPs', 'Internet IPs') and dest.resource IN (resource where role IN ('Instance))" -> define compliance standard -> Define recommendation for remediation & save.

C. In Policy Section-> Add Policy-> Network type -> Define Policy details Like Name.Severity-> Configure RQL query "network from vpc.flow_record where source.publicnetwork IN ('Suspicious IPs', 'Internet IPs') and dest.resource IN (resource where role IN (Instance))" -> define compliance standard -> Define recommendation for remediation & save.

D. In Policy Section-> Add Policy-> Network type -> Define Policy details Like Name.Severity-> Configure RQL query "config from network where source.network = UNTRUSTJNTERNET and dest.resource.type = 'Instance' and dest.cloud.type = 'AWS'" -> Define recommendation for remediation & save.

Answer: A

Explanation:

To create a network exposure policy that identifies instances accessible from any untrusted internet sources, a SecOps engineer would need to navigate to the Policy section within Prisma Cloud and add a new policy of the Config type. They would define the details of the policy such as the name and severity level and then configure the RQL query to specify conditions that match instances accessible from untrusted internet sources. The RQL query provided in the answer specifies that the source of the network traffic should be from an untrusted internet and that the destination resource should be an instance in the AWS cloud. After defining the compliance standards and providing recommendations for remediation, the policy can be saved to be enforced within the environment.

Question: 240

Which serverless cloud provider is covered by the "overly permissive service access" compliance check?

A. Alibaba

B. Azure

C. Amazon Web Services (AWS)

D. Google Cloud Platform (GCP)

Answer: C

Explanation:

The "overly permissive service access" compliance check is specifically designed to evaluate and ensure that cloud services are not granted more permissions than necessary, which could lead to potential security risks. Among the listed options, Amazon Web Services (AWS) is known for its extensive service offerings and the complexity of its Identity and Access Management (IAM) configurations. Prisma Cloud, a comprehensive cloud security platform by Palo Alto Networks, provides extensive support for AWS, including checks for overly permissive service access. This ensures that AWS environments adhere to the principle of least privilege, reducing the attack surface by limiting access to the minimum necessary to perform required tasks. Prisma Cloud's capabilities in AWS environments are detailed in various resources, including documentation and guides provided by Palo Alto Networks, which highlight its effectiveness in identifying and mitigating risks associated with excessive permissions in AWS services.

Question: 241

Console is running in a Kubernetes cluster, and Defenders need to be deployed on nodes within this cluster.

How should the Defenders in Kubernetes be deployed using the default Console service name?

A. From the deployment page in Console, choose "twistlock-console" for Console identifier, generate DaemonSet file, and apply DaemonSet to the twistlock namespace.

B. From the deployment page, configure the cloud credential in Console and allow cloud discovery to auto-protect the Kubernetes nodes.

C. From the deployment page in Console, choose "twistlock-console" for Console identifier and run the "curl | bash" script on the master Kubernetes node.

D. From the deployment page in Console, choose "pod name" for Console identifier, generate DaemonSet file, and apply the DaemonSet to twistlock namespace.

Answer: A

Explanation:

In Kubernetes environments, deploying Defenders to protect nodes involves leveraging DaemonSets, which ensure that every node in the cluster runs a copy of a specific pod. When the Console is running within a Kubernetes cluster, it's essential to correctly reference the Console service to ensure seamless communication between Defenders and the Console. Option A is the most straightforward and Kubernetes-native method for deploying Defenders. By choosing "twistlock-console" as the Console identifier on the deployment page within the Console, users can generate a DaemonSet configuration file tailored for the Twistlock namespace. This approach ensures that the Defenders are correctly configured to communicate with the Console, providing comprehensive security coverage across the Kubernetes nodes. This method aligns with best practices for deploying security agents in Kubernetes and is supported by Prisma Cloud (formerly Twistlock) documentation, which provides step-by-step instructions for deploying Defenders using DaemonSets.

Question: 242

Prisma Cloud supports sending audit event records to which three targets? (Choose three.)

A. SNMP Traps

B. Syslog

C. Stdout

D. Prometheus

E. Netflow

Answer: B,C,D

Explanation:

Question: 243

What factor is not used in calculating the net effective permissions for a resource in AWS?

A. AWS 1AM policy

B. Permission boundaries

C. IPTables firewall rule

D. AWS service control policies (SCPs)

Answer: C

Explanation:

In the context of calculating net effective permissions for a resource in AWS, IPTables firewall rule is not used. Net effective permissions in AWS are determined by evaluating various AWS-specific mechanisms such as IAM policies, permission boundaries, and service control policies (SCPs). IAM policies define what actions are allowed or denied for various AWS resources. Permission boundaries provide a way to delegate administration for IAM entities, setting the maximum permissions that an IAM entity can have. SCPs are part of AWS Organizations and allow for central control over the maximum available permissions for all accounts within an organization. IPTables, on the other hand, is a Linux-based application for setting up firewall rules on individual hosts and is not directly related to AWS resource permissions. Therefore, IPTables firewall rules are not considered when calculating net effective permissions in AWS, making option C the correct answer.

Question: 244

Which set of steps is the correct process for obtaining Console images for Prisma Cloud Compute Edition?

A. To retrieve Prisma Cloud Console images using basic authentication: 1. Access registry.twistlock.com and authenticate using "docker login."2. Retrieve the Prisma Cloud Console images using "docker pull."

B. To retrieve Prisma Cloud Console images using URL authentication:1. Access registry-url-auth.twistlock.com and authenticate using the user certificate.2. Retrieve the Prisma Cloud Console images using "docker pull."

C. To retrieve Prisma Cloud Console images using URL authentication: 1. Access registry- auth.twistlock.com and authenticate using the user certificate.2. Retrieve the Prisma Cloud Console images using "docker pull."

D. To retrieve Prisma Cloud Console images using basic authentication:1. Access registry.paloaltonetworks.com and authenticate using "docker login."2. Retrieve the Prisma Cloud Console images using "docker pull."

Answer: D

Explanation:

Prisma Cloud, part of Palo Alto Networks' cloud security suite, offers Console images that can be retrieved for deployment in various environments. The correct process for obtaining these images involves using basic authentication with Docker, a widely-used containerization platform. Users must first access the official Palo Alto Networks registry at registry.paloaltonetworks.com. Here, they are required to authenticate using the "docker login" command, which prompts for credentials. Upon successful authentication, users can then use the "docker pull" command to retrieve the Prisma Cloud Console images. This method ensures secure access to the latest Console images for deployment within an organization's infrastructure, aligning with best practices for container image management and deployment.

Question: 245

Which two integrated development environment (IDE) plugins are supported by Prisma Cloud as part of its Code Security? (Choose two.)

A. Visual Studio Code

B. IntelliJ

C. BitBucket

D. CircleCI

Answer: A,B

Explanation:

https://live.paloaltonetworks.com/t5/blogs/what-is-changing-for-ci-cd-plugins/ba-p/461676

Visual Studio Code IntelliJ IDEA https://live.paloaltonetworks.com/t5/blogs/what-is-changing-for-ci- cd-plugins/ba-p/461676

Question: 246

Which ban for DoS protection will enforce a rate limit for users who are unable to post five (5) ". tar.gz" files within five (5) seconds?

A. One with an average rate of 5 and file extensions match on ". tar.gz" on Web Application and API Security (WAAS)

B. One with an average rate of 5 and file extensions match on “. tar.gz" on Cloud Native Network Firewall (CNNF)

C. One with a burst rate of 5 and file extensions match on “. tar.gz" on Web Application and API Security (WAAS) *

D. One with a burst rate of 5 and file extensions match on “. tar.gz" on Cloud Native Network Firewall (CNNF)

Answer: A

Explanation:

In the context of DoS protection, enforcing a rate limit is a common strategy to prevent abuse and ensure service availability. The scenario described involves limiting the rate at which users can post ".tar.gz" files to five within five seconds. The correct ban configuration for this requirement would be one that specifies an average rate of 5 with a file extension match on “.tar.gz" within the Web Application and API Security (WAAS) component of a security solution like Prisma Cloud. WAAS is designed to protect web applications and APIs from various threats, including DoS attacks, by applying policies that can limit actions based on specific criteria, such as file types and request rates. This configuration ensures that any attempt to upload more than five ".tar.gz" files within a five- second window would be detected and blocked, mitigating the risk of DoS attacks targeting this particular file upload functionality.

Question: 247

Which two offerings will scan container images in Jenkins pipelines? (Choose two.)

A. Compute Azure DevOps plugin

B. Prisma Cloud Visual Studio Code plugin with Jenkins integration

C. Jenkins Docker plugin

D. Twistcli

E. Compute Jenkins plugin

Answer: D,E

Explanation:

https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/continuous_integration/jenkins_plugin.html

https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-

compute/continuous_integration/jenkins_pipeline_project

To scan container images in Jenkins pipelines, Prisma Cloud offers two specific tools:

D . Twistcli: This is a command-line interface tool provided by Prisma Cloud that allows users to scan container images for vulnerabilities and compliance issues. It can be integrated into Jenkins pipelines to automate the scanning process as part of the CI/CD workflow1.

E . Compute Jenkins plugin: This plugin integrates Prisma Cloud's capabilities directly into Jenkins, enabling automated scanning of container images during the build process. It provides a seamless way to include security checks within the Jenkins pipeline1.

Both Twistcli and the Compute Jenkins plugin are designed to work within the Jenkins environment to ensure that container images are scanned for security risks before they are deployed. By integrating these tools into the pipeline, developers can identify and address vulnerabilities early in the development cycle, contributing to a more secure software delivery process

Question: 248

What should be used to associate Prisma Cloud policies with compliance frameworks?

A. Compliance

B. Custom compliance

C. Alert rules

D. Policies

Answer: B

Explanation:

In the context of associating Prisma Cloud policies with compliance frameworks, the most appropriate option is "Custom compliance." Prisma Cloud provides a comprehensive set of security and compliance policies that can be applied to cloud environments. While predefined policies cover a wide range of compliance standards and best practices, every organization has unique requirements and may follow specific compliance frameworks that are not directly included in the predefined policies. Custom compliance allows organizations to define their own compliance frameworks and associate specific Prisma Cloud policies with these custom frameworks. This flexibility ensures that organizations can maintain compliance with their specific regulatory and industry standards, tailoring the Prisma Cloud policies to meet their unique compliance needs. Custom compliance frameworks can be created within Prisma Cloud to include a collection of policies that address the specific controls and requirements of the organization's chosen compliance standards, providing a tailored approach to cloud security and compliance.

Question: 249

Which three Orchestrator types are supported when deploying Defender? (Choose three.)

A. Red Hat OpenShift

B. Amazon ECS

C. Docker Swarm

D. Azure ACS

E. Kubernetes

Answer: A,B,E

Explanation:

Kubernetes, Openshift, ECS https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud- admin-compute/install/deploy-defender/orchestrator

Prisma Cloud supports integration with multiple orchestrators to facilitate the deployment of its Defender component in various environments. The supported orchestrators include Red Hat OpenShift, Amazon ECS, and Kubernetes. These platforms are supported because they provide robust environments for container orchestration, allowing Prisma Cloud to efficiently manage security operations across different cloud-native technologies.

Question: 250

Which three options for hardening a customer environment against misconfiguration are included in Prisma Cloud Compute compliance enforcement for hosts? (Choose three.)

A. Serverless functions

B. Docker daemon configuration

C. Cloud provider tags

D. Host configuration

E. Hosts without Defender agents

Answer: B,D,E

Explanation:

Prisma Cloud scans all hosts for compliance issues, provided that a defender is installed or the host is covered by an agentless scan. Among these, the following compliance issues are covered.

-Host configuration

-Docker daemon configuration

https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/compliance/host_scanning

Prisma Cloud Compute's compliance enforcement capabilities for hosts include ensuring proper configurations of Docker daemons and host operating systems, as well as managing hosts that do not have Defender agents installed. These measures are critical for hardening environments against misconfigurations which could lead to security vulnerabilities.

Question: 251

Creation of a new custom compliance standard that is based on other individual custom compliance standards needs to be automated.

Assuming the necessary data from other standards has been collected, which API order should be used for this new compliance standard?

A. 1) https://api.prismacloud.io/compliance/add2) https://api.prismacloud.io/compliance/requirementId/section3) https://api.prismacloud.io/compliance/complianceId/requirement

B. 1) https://api.prismacloud.io/compliance2) https://api.prismacloud.io/compliance/complianceId/requirement3) https://api.prismacloud.io/compliance/requirementId/section

C. 1) https://api.prismacloud.io/compliance/add2) https://api.prismacloud.io/compliance/complianceId/requirement3) https://api.prismacloud.io/compliance/requirementId/section

D. 1) https://api.prismacloud.io/compliance2)

https://api.prismacloud.io/compliance/requirementId/section3)

https://api.prismacloud.io/compliance/complianceId/requirement

Answer: B

Explanation:

https://api.prismacloud.io/compliance Add Compliance Standard

https://api.prismacloud.io/compliance/complianceId/requirement Add Compliance Requirement

https://api.prismacloud.io/compliance/requirementId/section Add Compliance Requirement Section

https://pan.dev/prisma-cloud/api/cspm/get-all-standards/

Question: 252

Which report includes an executive summary and a list of policy violations, including a page with details for each policy?

A. Compliance Standard

B. Business Unit

C. Cloud Security Assessment

D. Detailed

Answer: C

Explanation:

The Cloud Security Assessment report is a PDF report that summarizes the risks from open alerts in the monitored cloud accounts for a specific cloud type. The report includes an executive summary and a list of policy violations, including a page with details for each policy that includes the description and the compliance standards that are associated with it, the number of resources that passed and failed the check within the specified time period.

https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/manage-prisma- cloud-alerts/generate-reports-on-prisma-cloud-alerts

The report that includes an executive summary along with a list of policy violations and detailed pages for each policy is the "Cloud Security Assessment" report. This type of report is designed to provide organizations with a comprehensive overview of their cloud security posture, highlighting both compliance with security policies and areas needing attention.

Question: 253

A customer's Security Operations Center (SOC) team wants to receive alerts from Prisma Cloud via email once a day about all policies that have a violation, rather than receiving an alert every time a new violation occurs.

Which alert rule configuration meets this requirement?

A. Configure an alert rule with all the defaults except selecting email within the "Alert Notifications" tab and specifying recipient.

B. Configure an alert rule. Under the "Policies" tab, select "High Risk Severity Policies." In the "Set Alert Notifications" tab, select "Email > Recurring," set to repeat every 1 day, and enable "Email."

C. Set up email integrations under the "Integrations" tab in "Settings" and create a notification template.

D. Configure an alert rule. Under the "Policies" tab, select "All Policies." In the "Set Alert Notifications" tab, select "Email > Recurring," set to repeat every 1 day, and then enable "Email."

Answer: D

Explanation:

To receive daily email alerts for all policy violations, the SOC team should configure an alert rule that encompasses all policies and sets the notification frequency to once per day. This can be achieved by:

Navigating to the “Policies” tab within the alert rule configuration and selecting “All Policies” to ensure that the rule applies to every policy.

Moving to the “Set Alert Notifications” tab and choosing the “Email” notification method.

Setting the notification to “Recurring” with a frequency of every 1 day.

Enabling the email notification by specifying the recipient’s email address.

This configuration ensures that the SOC team will receive a consolidated email once a day that includes information on all

policies that have been violated, rather than receiving multiple alerts throughout the day as new violations occur. It allows the team to review the compliance status efficiently and prioritize their response accordingly.

Question: 254

Where can a user submit an external new feature request?

A. Aha

B. Help Center

C. Support Portal

D. Feature Request

Answer: A

Explanation:

https://prismacloud.ideas.aha.io/ideas

To submit an external new feature request for Prisma Cloud, users can utilize the Aha platform. By accessing the Palo Alto Networks Aha portal, users can submit their feature requests, suggest enhancements, and contribute to shaping the future of Prisma Cloud. Aha provides a structured way to collect and prioritize customer feedback, ensuring that valuable insights reach the product development teams.

For those seeking to propose new features or improvements, visiting the Aha portal and submitting their ideas is the recommended approach. It allows users to participate in the ongoing evolution of Prisma Cloud by sharing their requirements and vision for the platform

Question: 255

Which of the following is a reason for alert dismissal?

A. SNOOZED_AUTO_CLOSE

B. ALERT_RULE_ADDED

C. POLICY_UPDATED

D. USER_DELETED

Answer: C

Explanation:

https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/manage-prisma-cloud-alerts/prisma-cloud-alert-resolution-reasons

In Prisma Cloud, POLICY_UPDATED is a valid reason for the dismissal of an alert. This reason indicates that an alert can be dismissed if the policy that triggered the alert has been updated. When a policy is updated to no longer apply to certain resources or conditions, any open alerts that were generated based on the previous version of the policy may be dismissed as they are no longer relevant.

The other options, such as SNOOZED_AUTO_CLOSE, ALERT_RULE_ADDED, and USER_DELETED, are not standard reasons for the dismissal of an alert in Prisma Cloud. SNOOZED_AUTO_CLOSE refers to the temporary suspension of an alert, ALERT_RULE_ADDED is related to the creation of a new alert rule, and USER_DELETED would pertain to the removal of a user account, not directly to alert dismissal.

Question: 256

Which two statements explain differences between build and run config policies? (Choose two.)

A. Run and Network policies belong to the configuration policy set.

B. Build policies allow checking for security misconfigurations in the IaC templates and ensure these issues do not get into production.

C. Run policies monitor network activities in the environment and check for potential issues during runtime.

D. Run policies monitor resources and check for potential issues after these cloud resources are deployed.

Answer: B,D

Explanation:

The Run policies monitor resources and check for potential issues once these cloud resources are deployed Build policies enable you to check for security misconfigurations in the IaC templates and ensure that these issues do not make their way into production.

https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/prisma-cloud- policies/create-a-policy

B . Build policies: These are designed to identify insecure configurations in your Infrastructure as Code (IaC) templates, such as AWS CloudFormation, HashiCorp Terraform, and Kubernetes App manifests. The goal of build policies is to detect security issues early in the development process, before the actual resources are deployed in runtime environments. This helps ensure that security issues are identified and remediated before they can affect production1.

D . Run policies: These policies are focused on monitoring the deployed cloud resources and checking for potential issues during their operation. Run policies are essential for ongoing security and compliance in the production environment, as they provide visibility into the actual state of resources and their activities1.

Run and Network policies (A) are indeed part of the configuration policy set, but they do not highlight the difference between build and run policies. Similarly, while Run policies do monitor network activities ©, this statement does not contrast them with Build policies.

Question: 257

Which two CI/CD plugins are supported by Prisma Cloud as part of its Code Security? (Choose two.)

A. Checkov

B. Visual Studio Code

C. CircleCI

D. IntelliJ

Answer: A,C

Explanation:

https://live.paloaltonetworks.com/t5/blogs/what-is-changing-for-ci-cd-plugins/ba-p/461676

Prisma Cloud has announced changes to its CI/CD plugins due to the acquisition of Bridgecrew1. The existing IaC functionality in Prisma Cloud will be replaced by a Prisma “cloud code security” (CCS) module that delivers Bridgecrew integration in Prisma Cloud1. As part of this change, several CI/CD plugins that Prisma Cloud currently uses will either be replaced or modified1.

According to the information from the link, both Checkov and CircleCI are listed as integrations that will switch to the Prisma “cloud code security” (CCS) module1. Checkov is an open-source commandline interface (CLI) utility that includes more than 750 predefined policies and supports custom policies1. CircleCI is a continuous integration and continuous delivery platform1.

Question: 258

Which IAM RQL query would correctly generate an output to view users who enabled console access with both access keys and passwords?

A. config from network where api.name = ‘aws-iam-get-credential-report’ AND json.rule = cert_1_active is true or cert_2_active is true and password_enabled equals "true"

B. config from cloud.resource where api.name = 'aws-iam-get-credential-report' AND json.rule = access_key_1_active is true or access_key_2_active is true and password_enabled equals "true"

C. config from cloud.resource where api.name = 'aws-iam-get-credential-report’ AND json.rule = access_key_1_active is false or access_key_2_active is true and password_enabled equals "*"

D. config where api.name = ‘aws-iam-get-credential-report' AND json.rule= access_key_1_active is true or access_key_2_active is true and password_enabled equals “true”

Answer: B

Explanation:

View users who enabled console access with both access keys and passwords: config from cloud.resource where api.name = 'aws-iam-get-credential-report' AND json.rule = access_key_1_active is true or access_key_2_active is true and password_enabled is true https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-rql-reference/rql-reference/config-query/config-query-examples