Number: PCCSE
Passing Score: 800
Time Limit: 120
File Version: 5.5

Exam Code: PCCSE
Exam Name: Prisma Certified Cloud Security Engineer

Exam A

QUESTION 1
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.

Correct Answer: A
Section:
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.

QUESTION 2
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

Correct Answer: B, E
Section:
Explanation:
Prior to performing a rolling upgrade of Defenders, which are components responsible for enforcing security policies and protecting cloud workloads, one of the prerequisites is having an existing Console at version n-1 (option E). This ensures that the Console, which manages the Defenders, is compatible and can support the upgraded Defenders. A rolling upgrade allows for minimal disruption and ensures continuous protection during the upgrade process. The other options listed do not directly pertain to the prerequisites for a Defender rolling upgrade.

QUESTION 3
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.

Correct Answer: A
Section:

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 4
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

Correct Answer: C
Section:
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.

QUESTION 5
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

Correct Answer: B, C, D
Section:
Explanation:
For CI policy in image scanning with Jenkins or twistcli, options related to scoping include specifying credentials for accessing and scanning the images, setting conditions such as applying the rule only when vendor fixes are available to prioritize remediation efforts, and establishing failure thresholds to determine the severity levels that will cause the build to fail. These options focus on integrating security into the CI/CD pipeline, ensuring images are scanned for vulnerabilities, and enforcing security standards without hindering the development process. This approach aligns with best practices in DevSecOps by embedding security early in the development lifecycle, allowing for early detection and mitigation of vulnerabilities.

QUESTION 6

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

Correct Answer: B
Section:
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 7
Which port should a security team use to pull data from Console's API?

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

Correct Answer: C
Section:
Explanation:
Port 8084 is commonly used for accessing the Console's API in Prisma Cloud. This port allows security teams to programmatically interact with the Prisma Cloud Console, pulling data and automating various security and compliance tasks.

QUESTION 8
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 rule Select ''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 rule Select 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 rule Select one or more policies as part of the alert rule Add alert notifications Confirm the alert rule
D. Ensure the public cloud account is assigned to an account group Assign the confirmed account group to alert rule Select ''select all policies'' checkbox as part of the alert rule Add alert notifications Confirm the alert rule

Correct Answer: A
Section:
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 9
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:

Saml Missing Required Auto Provision Attributes
Error occurred due to unexpected value of required field 'SAML_RESPONSE'
Expected Value: 'unavailable'
Actual Value: '[ROLE=[3ed546ec-a509-4774-b872-e55cb2cfd60b]]'.

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.

Correct Answer: A
Section:
Explanation:
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 10
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

Correct Answer: B, D
Section:
Explanation:
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 11
Which policy type in Prisma Cloud can protect against malware?

A. Data
B. Config
C. Network
D. Event

Correct Answer: A
Section:
Explanation:
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 12

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

Correct Answer: B
Section:
Explanation:
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 13
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

Correct Answer: B
Section:
Explanation:
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 14
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

Correct Answer: D
Section:
Explanation:
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 15
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

Correct Answer: A
Section:
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.

QUESTION 16
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

Correct Answer: B
Section:
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 17
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.)

Select and Place:

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	

Correct Answer:

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

Section:
Explanation:

QUESTION 18
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

Correct Answer: B, C

Section:
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.
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 19
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

Correct Answer: A
Section:
Explanation:
Associating Prisma Cloud policies with compliance frameworks is done through the Custom Compliance feature in Prisma Cloud. This feature allows teams to map Prisma Cloud's out-of-the-box (OOTB) policies to various compliance standards and frameworks, thereby enabling organizations to tailor their compliance reporting and management according to specific regulatory requirements or internal compliance mandates.
Option A: Custom Compliance is the correct choice as it provides the flexibility to customize and align Prisma Cloud policies with an organization's specific compliance needs. It enables the compliance team to create custom compliance standards, map existing Prisma Cloud policies to these standards, and generate compliance reports that reflect the organization's unique compliance posture.
Prisma Cloud Compliance Documentation: Offers detailed guidance on setting up and managing custom compliance standards within Prisma Cloud, including how to associate policies with these standards.
Compliance Management Best Practices: Provides insights into effective compliance management strategies in cloud environments, emphasizing the role of customizable compliance frameworks to meet diverse regulatory requirements.

QUESTION 20
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.

Correct Answer: D
Section:
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.
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 21
Per security requirements, an administrator needs to provide a list of people who are receiving e-mails 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.

Correct Answer: D
Section:
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.
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 22
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>

Correct Answer: A
Section:
Explanation:
Scanning serverless functions for vulnerabilities and compliance issues is a critical aspect of securing serverless architectures. Prisma Cloud provides a CLI tool, twistcli, which supports scanning serverless function packages.
Option A: twistcli function scan <SERVERLESS_FUNCTION.ZIP> is the correct command for scanning serverless functions. This command allows users to scan the serverless function package (typically a ZIP file) for vulnerabilities, compliance issues, and other security concerns before deployment. By incorporating this scanning step into the CI/CD pipeline, organizations can ensure that their serverless functions are secure and compliant with relevant policies and standards before they are deployed to production.
Prisma Cloud twistcli Documentation: Provides comprehensive usage instructions for the twistcli tool, including commands for scanning serverless functions, container images, and IaC templates.
Serverless Security Best Practices: Discusses the unique security considerations for serverless architectures and the importance of pre-deployment scanning to identify and remediate potential security risks in serverless function code.

QUESTION 23
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.

Correct Answer: C
Section:
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.
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 24
What is an example of an outbound notification within Prisma Cloud?

A. AWS Inspector
B. Qualys
C. Tenable
D. PagerDuty

Correct Answer: D
Section:
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.
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 25
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

Correct Answer: B
Section:
Explanation:
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 26
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

Correct Answer: C
Section:
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 27
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.

Correct Answer: D
Section:
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.

QUESTION 28
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

Correct Answer: A, C, D

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

QUESTION 29
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''.

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

QUESTION 30
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'.

Correct Answer: A
Section:
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 31
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.

Correct Answer: C, D
Section:
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 32
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.

Correct Answer: D
Section:
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 33
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

Correct Answer: C
Section:
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 34
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.

Correct Answer: C
Section:
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 35
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.

Correct Answer: A, C
Section:
Explanation:
When an open alert from the previous day has been resolved without any configured auto-remediation, the change in alert status could be due to A. a user manually changing the alert status, indicating a manual intervention where someone reviewed and updated the alert status, and C. resource was deleted, implying that the resolution of the alert could be due to the removal of the resource associated with the alert, hence nullifying the alert condition.

QUESTION 36
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

Correct Answer: B, D, E
Section:
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 37
Which method should be used to authenticate to Prisma Cloud Enterprise programmatically?

A. single sign-on
B. SAML
C. basic authentication
D. access key

Correct Answer: D
Section:
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.

QUESTION 38
Which option shows the steps to install the Console in a Kubernetes Cluster?

A. Download the Console and Defender image Generate YAML for Defender Deploy Defender YAML using kubectl
B. Download and extract release tarball Generate YAML for Console Deploy 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

Correct Answer: B
Section:
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 39
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.

Correct Answer: D
Section:
Explanation:
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.

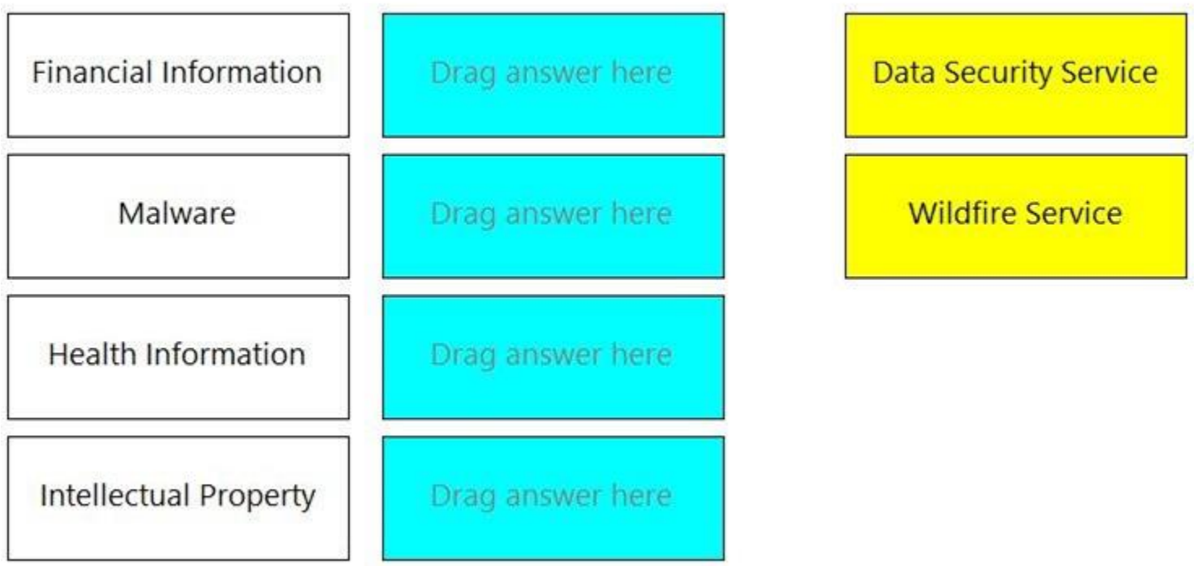
QUESTION 40
Which statement accurately characterizes SSO Integration on Prisma Cloud?

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.

Correct Answer: B
Section:
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 41
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.)

Select and Place:
Answer Area



Correct Answer:

Answer Area

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

QUESTION 42
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

Correct Answer: A, C
Section:
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 43
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

Correct Answer: A, B, D
Section:
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 44
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

Correct Answer: D
Section:
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 45
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

Correct Answer: D
Section:
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 46
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

Correct Answer: A, B
Section:
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.

QUESTION 47
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.

Correct Answer: D
Section:
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 non-root 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.
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 48
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

Correct Answer: B
Section:
Explanation:
To detect port scanning activities within an environment, a 'Port Scan' policy type (option B) would be the most appropriate. Port scanning is a technique used to identify open ports and services available on a host, often used by attackers to find vulnerabilities. A Port Scan policy is designed to detect and alert on such scanning activities, allowing security teams to take preventive measures. While Network (option A), Anomaly (option C), and Config (option D) policies play critical roles in cloud security, they do not specifically target the detection of port scanning behavior.

QUESTION 49
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

Correct Answer: B
Section:
Explanation:
In the deployment scenario described, where an NGINX container is listening on port 8080 and mapped to host port 80, the Cloud Native Application Firewall (CNAF) rule should specify host port 80 (option B) to protect the application. This is because the external traffic directed towards the containerized application will be accessing it through the host port 80, which is the exposed port to the outside network. Specifying port 80 in the CNAF rule ensures that the firewall can inspect and protect the incoming traffic to the application effectively.

QUESTION 50
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

Correct Answer: A, B, E
Section:
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 51
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

Correct Answer: D
Section:
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 52
One of the resources on the network has triggered an alert for a Default Config policy.
Given the following resource JSON snippet:

```
{
    "password_enabled": "false",
    "password_last_used": "N/A",
    "user_creation_time": "2021-02-09T06:56:33Z",
    "access_key_1_active": true,
    "access_key_2_active": false,
    "cert_1_last_rotated": "N/A",
    "cert_2_last_rotated": "N/A",
    "password_last_changed": "N/A",
    "password_next_rotation": "N/A",
    "access_key_1_last_rotated": "2021-02-09T06:57:20Z",
}
```

Which RQL detected the vulnerability?
A)

```
config from cloud.resource where api.name = 'aws-ecs-service' AND json.rule = launchType equals EC2 as X; config
from cloud.resource where api.name = 'aws-ecs-cluster' AND json.rule = status equals ACTIVE and
registeredContainerInstancesCount equals 0 as Y; filter '$.X.ckusterArn equals $.Y.clusterArn'; show Y;
```

B)

```
config from cloud.resource where cloud.type = 'aws' and api.name = 'aws-iam-get-credential-report' AND json.rule
= '(access_key_1_active is true and access_key_1_last_rotated != N/A and
_DateTime.ageInDays(access_key_1_last_rotated) > 90) or (access_key_2_active is true and
access_key_2_last_rotated != N/A and _DateTime.ageInDays(access_key_2_last_rotated) > 90)'
```

C)

```
config from cloud.resource where cloud.type = 'aws' AND api.name ='aws-ec2-describe-images' AND json.rule =
image.platform contains windows and image.imageId contains ami-1e542176
```

D)

```
config from cloud.resource where cloud.type = 'aws' AND api.name ='aws-ec2-describe-secutity-groups' AND
json.rule = isShared is false and (ipPermissions[?any((ipProtocol equals tcp or ipProtocol equals icmp or
ipProtocol equals icmpv6 or ipProtocol equals udp) and (ipRanges[*] contains 0.0.0.0/0 or ipv6Ranges[*].cidrIpv6
```

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

Correct Answer: B
Section:
Explanation:
The correct RQL (Resource Query Language) that detected the vulnerability is:
config from cloud.resource where cloud.type = 'aws' and api.name = 'aws-iam-get-credential-report' AND json.rule = '(access_key_1_active is true and access_key_1_last_rotated != N/A and DateTime. ageInDays (access_key_1_last_rotated) > 90) or (access_key_2_active is true and access_key_2_last_rotated != N/A and _DateTime. ageInDays (access_key_2_last_rotated) > 90)'
This RQL is designed to check the age of the AWS IAM user's access keys to ensure that they are rotated within a recommended period, typically 90 days. If the access keys have not been rotated within this timeframe, it would be considered a security risk or vulnerability, as old keys may potentially be compromised. By enforcing access key rotation, it minimizes the risk of unauthorized access.
The reference for this type of policy check can be seen in cloud security best practices that advocate for regular rotation of access keys to minimize the potential impact of key compromise. CSPM tools like Prisma Cloud include such checks to automate compliance with these best practices.

QUESTION 53
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

Correct Answer: D
Section:
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 54

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

Correct Answer: C
Section:
Explanation:
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 55
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.

Correct Answer: D
Section:
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

QUESTION 56
Which API calls can scan an image named myimage: latest with twistcli and then retrieve the results from Console?

A. $ twistcli images scan \ --address <COMPUTE_CONSOLE> \ --user <COMPUTER_CONSOLE_USER> \ --password <COMPUTER_CONSOLE_PASSWD> \ --verbose \ myimage: latest
B. $ twistcli images scan \ --address <COMPUTE_CONSOLE> \ --user <COMPUTER_CONSOLE_USER> \ --password <COMPUTER_CONSOLE_PASSWD> \ --details \ myimage: latest
C. $ twistcli images scan \ --address <COMPUTE_CONSOLE> \ --user <COMPUTER_CONSOLE_USER> \ --password <COMPUTER_CONSOLE_PASSWD> \ myimage: latest
D. $ twistcli images scan \ --address <COMPUTE_CONSOLE> \ --user <COMPUTER_CONSOLE_USER> \ --password <COMPUTER_CONSOLE_PASSWD> \ --console \ myimage: latest

Correct Answer: C
Section:
Explanation:
The API calls that can scan an image named myimage: latest with twistcli and then retrieve the results from Console do not require any additional flags beyond the address, user, and password for the Prisma Cloud Compute

console. The --verbose, --details, and --console flags are not necessary for performing the scan and retrieving the results. The twistcli command with the required parameters initiates the scan, and upon completion, the results are available in the Prisma Cloud Compute console for review.
Reference to this process is provided in the Prisma Cloud Compute documentation, which outlines the steps for scanning container images with the twistcli command-line tool and retrieving the results from the Compute Console for analysis and action.

QUESTION 57
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.iam.v1.SetIamPolicyRequest", "policy": { "bindings": [
```

B)

```
], "stateTransitionReason": "", "elasticGpuAssociations": [], "capacityReservationSpecification": {
 "capacityReservationPreference": "open" }, "elasticInferenceAcceleratorAssociations": []
```

C)

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

D)

```
"payload": { "requestMetadata": { "callerSuppliedUserAgent": "Terraform/0.14.0
(+https://www.terraform.io) Terrafom-Plugin-SDK/2.1.0 terraform-provider-google/3.50.0,gzip(gfe)",
 "callerIp": "34.265.226.252" }, "request": { "@type":
"type.googleapis.com/compute.disks.createSnapshot" },
```

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

Correct Answer: C
Section:
Explanation:
The given RQL (Resource Query Language) query is looking for specific audit events related to cryptographic key actions and snapshot creation. The snippet that matches this query is Option C, which contains the statement indicating permissions that allow any action ('Action': '*') and the reference to the version date '2012-10-17' that corresponds to the policy within the audit log.
This can be cross-referenced with cloud provider documentation, such as AWS CloudTrail or Google Cloud Audit Logs, which record user activities and API usage. The RQL provided would be used in a CSPM tool to query these audit logs for the specified events.

QUESTION 58
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

Correct Answer: C, D
Section:
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 59
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.

Correct Answer: B
Section:
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.

QUESTION 60
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.

Correct Answer: C
Section:
Explanation:
To enable role-based access control (RBAC) for the Docker engine in a Prisma Cloud environment, the first configuration step involves setting Docker's listener type to TCP. This change allows Docker to accept connections over the network, facilitating the integration with Prisma Cloud Defenders, which can then enforce RBAC policies. Configuring Docker to listen on TCP is essential for enabling communication between the Docker daemon and Prisma Cloud Defenders, which act as the enforcement point for RBAC, controlling which users or services can perform actions on the Docker engine based on their roles and permissions. This setup is foundational for implementing granular access controls and enhancing the security of Docker operations within the environment.

QUESTION 61
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

Correct Answer: D
Section:
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 62
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

Correct Answer: B
Section:
Explanation:
In the context of Prisma Cloud and its Container Runtime Model, the Learning phase is a crucial period where the system observes and understands the normal behaviors and patterns of container activities. This 'dry run' period allows Prisma Cloud to establish a baseline of what is considered normal, which later helps in identifying anomalies or malicious activities. A 48-hour period is typically used for this learning phase to ensure that a sufficient amount of data is collected across various times and conditions, providing a comprehensive understanding of typical container operations.

QUESTION 63
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

Correct Answer: A, D, E
Section:
Explanation:
The Incident Explorer section in Runtime Defense of a cloud security platform like Prisma Cloud is designed to reflect various types of security incidents that might occur within a containerized environment. Incident types such as Crypto miners, Port Scanning, and SQL Injection are common threats that are actively monitored. Crypto miners indicate unauthorized cryptocurrency mining activities; Port Scanning involves scanning a computer network or a single machine for open ports, which could be a precursor to more serious attacks; and SQL Injection is a code injection technique that might be used to attack data-driven applications. These incident types are critical to monitor for maintaining the security and integrity of cloud and container environments.

QUESTION 64
Which two filters are available in the SecOps dashboard? (Choose two.)

A. Time range
B. Account Groups
C. Service Name
D. Cloud Region

Correct Answer: A, B
Section:
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 65
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

Correct Answer: B
Section:
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 66
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

Correct Answer: A
Section:
Explanation:
In the Anomaly settings of a cloud security platform, choosing a High alert disposition severity is crucial when the objective is to generate alerts for both low and high severity incidents, especially in scenarios such as reporting unknown browsers and OS, impossible time travel, or account hijacking attempts. Setting the alert severity to High ensures that the security team is promptly notified of both overt and subtle anomalies, enabling quick response to potential security threats that may indicate unauthorized access or suspicious activities within the cloud environment.

QUESTION 67
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

Correct Answer: B

Section:
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 68
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.

Correct Answer: C
Section:
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

QUESTION 69
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

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

QUESTION 70
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

Correct Answer: B
Section:
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.

QUESTION 71
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

Correct Answer: A, B
Section:
Explanation:
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 72
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.

Correct Answer: D
Section:
Explanation:
Prisma Cloud Compute offers native integration capabilities with Splunk, a leading platform for operational intelligence and security information and event management (SIEM). By enabling the Splunk option within the Prisma Cloud Console, administrators can seamlessly forward Console and Defender logs to Splunk. This integration facilitates advanced analytics, real-time monitoring, and comprehensive incident response workflows within Splunk, leveraging the detailed security data provided by Prisma Cloud Compute.

QUESTION 73
The security team wants to enable the ''block'' option under compliance checks on the host.
What effect will this option have if it violates the compliance check?

A. The host will be taken offline.
B. Additional hosts will be prevented form starting.
C. Containers on a host will be stopped.
D. No containers will be allowed to start on that host.

Correct Answer: D

Section:
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.

QUESTION 74
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.

Correct Answer: D
Section:
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 75
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.

Correct Answer: C
Section:
Explanation:
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 76
Which RQL query type is invalid?

A. Event
B. IAM
C. Incident
D. Config

Correct Answer: C

Section:
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 77
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

Correct Answer: B
Section:
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 78
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

Correct Answer: A, D
Section:
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 79
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

Correct Answer: A
Section:
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.

QUESTION 80
How often do Defenders share logs with Console?

A. Every 10 minutes
B. Every 30 minutes
C. Every 1 hour
D. Real time

Correct Answer: D
Section:
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 81
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

Correct Answer: B
Section:
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 82
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

Correct Answer: B, D, E
Section:
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 83
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

Correct Answer: A
Section:
Explanation:
To retrieve compliance policies for images scanned in a continuous integration (CI) pipeline via Prisma Cloud's API, the correct endpoint to use is GET /api/v22.01/policies/compliance (A). This endpoint provides access to the comprehensive list of compliance policies defined within Prisma Cloud, including those applicable to images in the CI pipeline. It allows administrators to programmatically retrieve and review the policies to ensure that images meet the organization's compliance standards before they are deployed. The other options (B, C, D) specify endpoints that do not match the standard API endpoint format used by Prisma Cloud for accessing compliance policies, making them incorrect.

QUESTION 84
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.

Correct Answer: A
Section:
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 85
Anomaly policy uses which two logs to identify unusual network and user activity? (Choose two.)

A. Network flow
B. Audit
C. Traffic
D. Users

Correct Answer: A, B
Section:
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 86
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

Correct Answer: A, D
Section:
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 87
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.

Correct Answer: A
Section:
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 88
Which two integrations enable ingesting host findings to generate alerts? (Choose two.)

A. Splunk
B. Tenable
C. JIRA
D. Qualys

Correct Answer: B, D

Section:
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.

QUESTION 89
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

Correct Answer: B
Section:
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 90
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.

Correct Answer: D
Section:
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 91
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.

Correct Answer: B
Section:

Explanation:
When a role is deleted in Prisma Cloud, it directly impacts any integrations that rely on the access key associated with that role. These integrations use the access key to authenticate and make API calls to Prisma Cloud for various operations. Deleting the role invalidates the access key, causing these integrations to lose their ability to communicate with Prisma Cloud, leading to a cessation of their functionality until a new role with a valid access key is configured. This underscores the importance of carefully managing roles and access keys to avoid disrupting integrated systems and services.

QUESTION 92
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. Offline alert

Correct Answer: B
Section:
Explanation:
To receive notifications about alerts generated when the operator is away from the Prisma Cloud Console, a Notification rule must be created. Notification rules in Prisma Cloud are designed to define the conditions under which notifications are sent and to specify the recipients of these notifications. These rules can be configured to trigger notifications based on various criteria, such as the severity of alerts, specific types of security incidents, or compliance violations. By setting up notification rules, operators can ensure that they are promptly informed of critical security events, even when they are not actively monitoring the Prisma Cloud Console, enabling timely investigation and response to potential security issues.

QUESTION 93
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'

Correct Answer: A
Section:
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 94
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.

Correct Answer: A, C
Section:
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 95
Which field is required during the creation of a custom config query?

A. resource status
B. api.name
C. finding.type
D. cloud.type

Correct Answer: B
Section:
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 96
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

Correct Answer: B
Section:
Explanation:
The role that should be assigned to DevOps users who need access to deploy Container and Host Defenders in Compute within Prisma Cloud is typically 'Build and Deploy Security.' This role is designed to provide the necessary permissions for users involved in the development and deployment phases of the application lifecycle. It allows them to integrate security measures, such as deploying Container and Host Defenders, into their workflows. By having this role, DevOps teams can ensure that security is embedded into the build and deployment processes, helping to maintain the security of containerized and host-based applications from the outset.

QUESTION 97
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

Correct Answer: B, D, E
Section:
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 98
Which two attributes are required for a custom config RQL? (Choose two.)

A. json.rule
B. cloud.account
C. api.name
D. tag

Correct Answer: A, C
Section:
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 99
Which type of query is used for scanning Infrastructure as Code (IaC) templates?

A. API
B. XML
C. JSON
D. RQL

Correct Answer: D
Section:
Explanation:
In Prisma Cloud, the Resource Query Language (RQL) is used as a sophisticated querying language that enables deep inspection and analysis of cloud resources, configurations, and metadata. RQL is particularly adept at scanning Infrastructure as Code (IaC) templates because it allows for granular querying of cloud resources and their attributes, including those defined within IaC templates such as Terraform and CloudFormation. This capability is essential for identifying potential security risks, misconfigurations, and compliance issues within the infrastructure code before it's deployed, ensuring that cloud environments are secure from the outset.

QUESTION 100
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

Correct Answer: B
Section:
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 101
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

Correct Answer: D
Section:
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 102
Which Prisma Cloud policy type can protect against malware?

A. Event
B. Network
C. Config
D. Data

Correct Answer: D
Section:
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 103
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.

Correct Answer: D
Section:
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.

QUESTION 104
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

Correct Answer: A, D
Section:
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 105
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.

Correct Answer: A
Section:
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 106
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

Correct Answer: A, D
Section:
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 107
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)

Correct Answer: A
Section:
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.