Cloud Security Engineer Certified Official Practice Test PCCSE - May-2024 [Q88-Q102

Cloud Security Engineer Certified Official Practice Test PCCSE - May-2024 Ace Palo Alto Networks PCCSE Certification with Actual Questions May 31, 2024 Updated

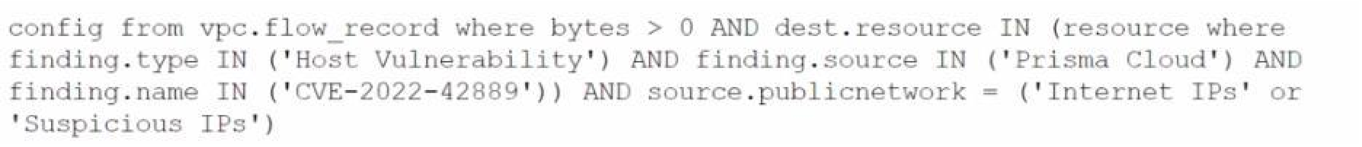
The PCCSE exam consists of 65 multiple-choice questions and is designed to test a candidate's proficiency in using Prisma Cloud to secure cloud environments. PCCSE exam covers a range of topics, including cloud security fundamentals, cloud governance, compliance management, network security, workload protection, data security, and threat detection and response. Candidates must pass the exam with a score of at least 70% to earn the PCCSE certification.

Q88. Based on the following information, which RQL query will satisfy the requirement to identify VM hosts deployed to organization public cloud environments exposed to network traffic from the internet and affected by Text4Shell RCE (CVE-2022-42889) vulnerability?

* Network flow logs from all virtual private cloud (VPC) subnets are ingested to the Prisma Cloud Enterprise Edition tenant.

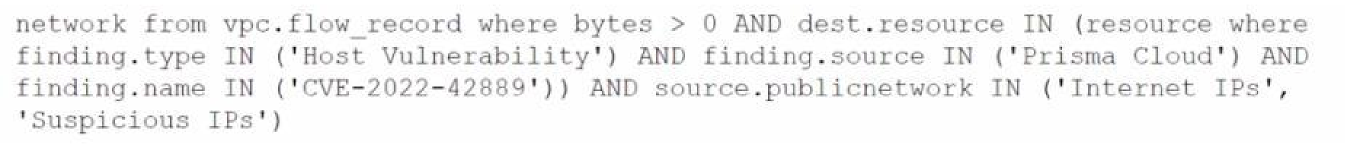
* All virtual machines (VMs) have Prisma Cloud Defender deployed.

*



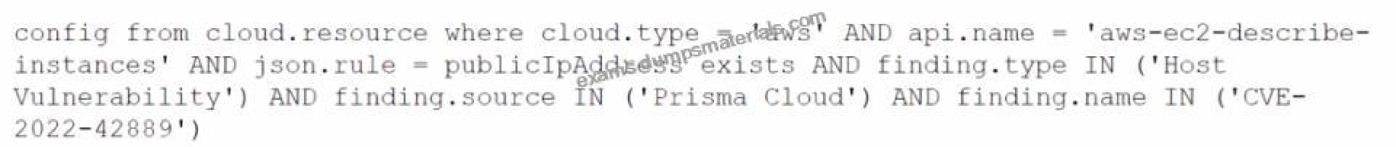
```
config from vpc.flow_record where bytes > 0 AND dest.resource IN (resource where
finding.type IN ('Host Vulnerability') AND finding.source IN ('Prisma Cloud') AND
finding.name IN ('CVE-2022-42889')) AND source.publicnetwork = ('Internet IPs' or
'Suspicious IPs')
```

*



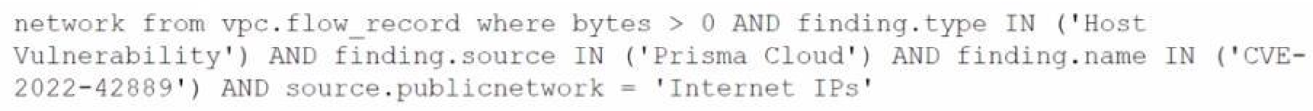
```
network from vpc.flow_record where bytes > 0 AND dest.resource IN (resource where
finding.type IN ('Host Vulnerability') AND finding.source IN ('Prisma Cloud') AND
finding.name IN ('CVE-2022-42889')) AND source.publicnetwork IN ('Internet IPs',
'Suspicious IPs')
```

*



```
config from cloud.resource where cloud.type = 'aws' AND api.name = 'aws-ec2-describe-
instances' AND json.rule = publicIpAddress exists AND finding.type IN ('Host
Vulnerability') AND finding.source IN ('Prisma Cloud') AND finding.name IN ('CVE-
2022-42889')
```

*



```
network from vpc.flow_record where bytes > 0 AND finding.type IN ('Host
Vulnerability') AND finding.source IN ('Prisma Cloud') AND finding.name IN ('CVE-
2022-42889') AND source.publicnetwork = 'Internet IPs'
```

The RQL query in Option A is designed to identify VM hosts that are exposed to internet traffic and are affected by the Text4Shell RCE vulnerability (CVE-2022-42889). This query looks for network flow records with byte transfers indicating activity and filters for resources with host vulnerability findings sourced from &#8216;Prisma Cloud&#8217;. It also checks for exposure to suspicious or internet IPs, satisfying the criteria for the given scenario.

Q89. The Unusual protocol activity (Internal) network anomaly is generating too many alerts. An administrator has been asked to tune it to the option that will generate the least number of events without disabling it entirely.

Which strategy should the administrator use to achieve this goal?
* Disable the policy
* Set the Alert Disposition to Conservative
* Change the Training Threshold to Low
* Set Alert Disposition to Aggressive
Section: (none)

Explanation

Q90. The development team wants to block Cross Site Scripting attacks from pods in its environment. How should the team construct the CNAF policy to protect against this attack?
* create a Host CNAF policy, targeted at a specific resource, check the box for XSS attack protection, and set the action to &#8220;prevent&#8221;.
* create a Container CNAF policy, targeted at a specific resource, check the box for XSS attack protection, and set the action to alert.
* create a Container CNAF policy, targeted at a specific resource, check the box for XSS protection, and set the action to prevent.
* create a Container CNAF policy, targeted at a specific resource, and they should set &#8220;Explicitly allowed inbound IP sources&#8221; to the IP address of the pod.

Q91. 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&#8217;s request?
* Trusted Login IP Addresses
* Anomaly Trusted List
* Trusted Alert IP Addresses
* Enterprise Alert Disposition
Section: (none)

Explanation

Q92. Which field is required during the creation of a custom config query?
* cloud.type
* resource status
* finding.type
* api.name

Q93. During the Learning phase of the Container Runtime Model, Prisma Cloud enters a &#8220;dry run&#8221; period for how many hours?
* 1
* 24
* 48
* 4

Q94. What is an automatically correlated set of individual events generated by the firewall and runtime sensors to identify unfolding attacks?
* policy
* incident
* audit
* anomaly

Q95. Which two filters are available in the SecOps dashboard? (Choose two.)
* Time range
* Account Groups
* Service Name
* Cloud Region
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.

Q96. Web-Application and API Security (WAAS) provides protection for which two protocols? (Choose two.)
* Tomcat Web Connector via AJP
* HTTP
* SSH
* TLS

Q97. Which role must be assigned to DevOps users who need access to deploy Container and Host Defenders in Compute?
* Cloud Provisioning Admin

* Build and Deploy Security
* System Admin
* Developer

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 &#8220;Build and Deploy Security.&#8221; 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.

Q98. The development team is building pods to host a web front end, and they want to protect these pods with an application firewall.

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

Q99. 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&#8217;s associated permission levels, in a Prisma Cloud Enterprise tenant.

Which public documentation location should be reviewed to help determine the required attributes to carry out this step?
* Prisma Cloud Administrator&#8217;s Guide (Compute)
* Prisma Cloud API Reference
* Prisma Cloud Compute API Reference
* Prisma Cloud Enterprise Administrator&#8217;s Guide

Q100. What are two built-in RBAC permission groups for Prisma Cloud? (Choose two.)
* Group Membership Admin
* Group Admin
* Account Group Admin
* Account Group Read Only

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

Q101. Which data security default policy is able to scan for vulnerabilities?
* Objects containing Vulnerabilities
* Objects containing Threats
* Objects containing Malware
* Objects containing Exploits

The data security default policy capable of scanning for vulnerabilities is &#8220;Objects containing Malware&#8221;. In cloud security, malware scanning is an essential feature of CSPM tools that allows for the identification of malicious software within objects stored in the cloud. A policy that scans for objects containing malware ensures that any files or code bases in the cloud environment are examined for potential threats, protecting the cloud resources from being compromised.

Q102. 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?

* add a new runtime policy targeted at a specific Container name, add ransomWare process into the denied process list and set the action to &#8220;prevent&#8221;.
* choose &#8220;copy into rule&#8221; for the Container add a ransomWare process into the denied process list and set the action to &#8220;block&#8221;
* set the Container model to manual relearn and set the default runtime rule to block for process protection.
* set the Container model to relearn and set the default runtime rule to prevent for process protection.

The PCCSE exam is a vendor-neutral certification program that is recognized globally by industry professionals and employers alike. It is designed to test the knowledge and skills of security professionals who work with cloud security solutions, particularly those who work with Prisma. PCCSE exam is intended to ensure that candidates have a strong understanding of cloud security best practices, as well as the technical skills required to implement and manage cloud security solutions using Prisma.

Try Free and Start Using Realistic Verified PCCSE Dumps Instantly.:
https://www.dumpsmaterials.com/PCCSE-real-torrent.html]