PCCSE$^{\text{Q\&As}}$

Prisma Certified Cloud Security Engineer

Pass Palo Alto Networks PCCSE Exam with 100% Guarantee

QUESTION 1

Which RQL query is used to detect certain high-risk activities executed by a root user in AWS?

A. event from cloud.audit_logs where operation IN (\\'ChangePassword\\', \\'ConsoleLogin\\', \\'DeactivateMFADevice\\', \\'DeleteAccessKey\\' , \\'DeleteAlarms\\') AND user = \\'root\\'

B. event from cloud.security_logs where operation IN (\\'ChangePassword\\', \\'ConsoleLogin\\', \\'DeactivateMFADevice\\', \\'DeleteAccessKey\\' , \\'DeleteAlarms\\') AND user = \\'root\\'

C. config from cloud.audit_logs where operation IN (\\'ChangePassword\\', \\'ConsoleLogin\\', \\'DeactivateMFADevice\\', \\'DeleteAccessKey\\', \\'DeleteAlarms\\') AND user = \\'root\\'

D. event from cloud.audit_logs where Risk.Level = \\'high\\' AND user = \\'root\\'

Correct Answer: A

https://docs.prismacloud.io/en/classic/rql-reference/rql-reference/event-query/event-query-examples https://docs.prismacloud.io/en/classic/rql-reference/rql-reference/event-query/event-query-examples#idda895fd2-4496-4b31-9766-7d50215dcc18

QUESTION 2

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

QUESTION 3

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

QUESTION 4

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 (CVE2022-42889) vulnerability?

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

A. 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\\')

B. 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\\')

C. 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\\'

D. 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\\')

Correct Answer: A

QUESTION 5

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

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

Latest PCCSE Dumps PCCSE VCE Dumps PCCSE Practice Test