Prisma Certified Cloud Security Engineer

1. Given a default deployment of Console, a customer needs to identify the alerted compliance checks that are set by default.
Where should the customer navigate in Console?

A. Monitor > Compliance

B. Defend > Compliance

C. Manage > Compliance

D. Custom > Compliance

Answer(s): B

---

2. Which container scan is constructed correctly?

A. twistcli images scan -u api -p api --address https://us-west1.cloud.twistlock.com/us-3-123456789 --container myimage/latest

B. twistcli images scan --docker-address https://us-west1.cloud.twistlock.com/us-3-123456789 myimage/latest

C. twistcli images scan -u api -p api --address https://us-west1.cloud.twistlock.com/us-3-123456789 - -details myimage/latest

D. twistcli images scan -u api -p api --docker-address https://us-west1.cloud.twistlock.com/us-3-123456789 myimage/latest

Answer(s): C

---

3. The development team wants to fail CI jobs where a specific CVE is contained within the image. How should the development team configure the pipeline or policy to produce this outcome?

A. Set the specific CVE exception as an option in Jenkins or twistcli.

B. Set the specific CVE exception as an option in Defender running the scan.

C. Set the specific CVE exception as an option using the magic string in the Console.

D. Set the specific CVE exception in Console's CI policy.

Answer(s): D

---

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

- ☐ A. Personally identifiable information
- ☐ B. Malicious IP
- ☐ C. Compliance standard
- ☐ D. Financial information
- ☐ E. Malware

Answer(s): A C D

---

5. A customer has a requirement to terminate any Container from image topSecret:latest when a process named ransomWare is executed.
How should the administrator configure Prisma Cloud Compute to satisfy this requirement?

A. set the Container model to manual relearn and set the default runtime rule to block for process protection.

B. set the Container model to relearn and set the default runtime rule to prevent for process protection.

C. add a new runtime policy targeted at a specific Container name, add ransomWare process into the denied process list, and set the action to "prevent".

D. choose "copy into rule" for the Container, add a ransomWare process into the denied process list, and set the action to "block".

Answer(s): C

---

6. Which statement is true about obtaining Console images for Prisma Cloud Compute Edition?

A. To retrieve Prisma Cloud Console images using basic auth:1. Access registry.paloaltonetworks.com, and authenticate using `docker login'.2. Retrieve the Prisma Cloud Console images using `docker pull'.

B. To retrieve Prisma Cloud Console images using basic auth:1. Access registry.twistlock.com, and authenticate using `docker login'.2. Retrieve the Prisma Cloud Console images using `docker pull'.

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

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

Answer(s): A

---

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

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

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

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

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

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

Answer(s): C D

---

8. A security team notices a number of anomalies under Monitor > Events. The incident response team works with the developers to determine that these anomalies are false positives.
What will be the effect if the security team chooses to Relearn on this image?

A. The model is deleted, and Defender will relearn for 24 hours.

B. The anomalies detected will automatically be added to the model.

C. The model is deleted and returns to the initial learning state.

D. The model is retained, and any new behavior observed during the new learning period will be added to the existing model.

Answer(s): D

---

9. A customer does not want alerts to be generated from network traffic that originates from trusted internal networks.
Which setting should you use to meet this customer's request?

A. Trusted Login IP Addresses

B. Anomaly Trusted List

C. Trusted Alert IP Addresses

D. Enterprise Alert Disposition

Answer(s): C

---

10. A DevOps lead reviewed some system logs and notices some odd behavior that could be a data exfiltration attempt. The DevOps lead only has access to vulnerability data in Prisma Cloud Compute, so the DevOps lead passes this information to SecOps.

Which pages in Prisma Cloud Compute can the SecOps lead use to investigate the runtime aspects of this attack?

A. The SecOps lead should investigate the attack using Vulnerability Explorer and Runtime Radar.

B. The SecOps lead should use Incident Explorer and Compliance Explorer.

C. The SecOps lead should use the Incident Explorer page and Monitor > Events > Container Audits.

D. The SecOps lead should review the vulnerability scans in the CI/CD process to determine blame.

Answer(s): C

---

11. A customer finds that an open alert from the previous day has been resolved. No auto-remediation was configured.
Which two reasons explain this change in alert status? (Choose two.)

☐ A. user manually changed the alert status.

☐ B. policy was changed.

☐ C. resource was deleted.

☐ D. alert was sent to an external integration.

Answer(s): A C

---

12. Which three steps are involved in onboarding an account for Data Security? (Choose three.)

☐ A. Create a read-only role with in-line policies

☐ B. Create a Cloudtrail with SNS Topic

☐ C. Enable Flow Logs

☐ D. Enter the RoleARN and SNSARN

☐ E. Create a S3 bucket

Answer(s): B D E

---

13. An administrator has deployed Console into a Kubernetes cluster running in AWS. The administrator also has configured a load balancer in TCP passthrough mode to listen on the same ports as the default Prisma Compute Console configuration.
In the build pipeline, the administrator wants twistcli to talk to Console over HTTPS.
Which port will twistcli need to use to access the Prisma Compute APIs?

A. 8084

B. 443

C. 8083

D. 8081

Answer(s): A

---

14. A customer is reviewing Container audits, and an audit has identified a cryptominer attack.
Which three options could have generated this audit? (Choose three.)

☐ A. The value of the mined currency exceeds $100.

☐ B. High CPU usage over time for the container is detected.

☐ C. Common cryptominer process name was found.

☐ D. The mined currency is associated with a user token.

☐ E. Common cryptominer port usage was found.

Answer(s): B C E

---

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

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

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

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

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

Answer(s): D

---

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

□ A. enable flow logs for Prisma Cloud.

□ B. create the Prisma Cloud role.

□ C. enable the required APIs for Prisma Cloud.

□ D. publish the flow log to a storage bucket.

Answer(s): B C

---

17. Which statement about build and run policies is true?

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

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

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

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

Answer(s): A

---

18. An administrator sees that a runtime audit has been generated for a host. The audit message is:
"Service postfix attempted to obtain capability SHELL by executing /bin/sh /usr/libexec/postfix/postfix- script.stop. Low severity audit, event is automatically added to the runtime model"
Which runtime host policy rule is the root cause for this runtime audit?

A. Custom rule with specific configuration for file integrity

B. Custom rule with specific configuration for networking

C. Default rule that alerts on capabilities

D. Default rule that alerts on suspicious runtime behavior

Answer(s): D

---

19. Which option identifies the Prisma Cloud Compute Edition?

A. Package installed with APT

B. Downloadable, self-hosted software

C. Software-as-a-Service (SaaS)

D. Plugin to Prisma Cloud

Answer(s): B

---

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

A. Host

B. Container

C. Functions

D. Image

Answer(s): D