ATMIC NETWORKS
YOUR GUIDE TO GLOBAL CERTIFIATION

"Please note that these files may not be up to date. However, the questions will help you understand the exam format and typical question patterns."

www.atmicnetworks .com

Warning: Keep connected with our support team for latest updates

Question: 1

Which standard approach to security is augmented by the 4C's of Cloud Native security?

A. Zero Trust

B. Least Privilege

C. Defense-in-Depth

D. Secure-by-Design

Answer: C

Question: 2

In a Kubernetes cluster, what are the security risks associated with using ConfigMaps for storing secrets?

A. Storing secrets in ConfigMaps does not allow for fine-grained access control via RBAC.

B. Storing secrets in ConfigMaps can expose sensitive information as they are stored in plaintext and can be accessed by unauthorized users.

C. Using ConfigMaps for storing secrets might make applications incompatible with the Kubernetes cluster.

D. ConfigMaps store sensitive information in etcd encoded in base64 format automatically, which does not ensure confidentiality of data.

Answer: B, D

Question: 3

What is the difference between gVisor and Firecracker?

A. gVisor is a user-space kernel that provides isolation and security for containers. At the same time, Firecracker is a lightweight virtualization technology for creating and managing secure, multi-tenant container and function-as-a-service (FaaS) workloads.

B. gVisor is a lightweight virtualization technology for creating and managing secure, multi-tenant container and function-as-a-service (FaaS) workloads. At the same time, Firecracker is a user-space kernel that provides isolation and security for containers.

C. gVisor and Firecracker are both container runtimes that can be used interchangeably.

D. gVisor and Firecracker are two names for the same technology, which provides isolation and security for containers.

Answer: A

Question: 4

You want to minimize security issues in running Kubernetes Pods. Which of the following actions can help achieve this goal?

A. Sharing sensitive data among Pods in the same cluster to improve collaboration.

B. Running Pods with elevated privileges to maximize their capabilities.

C. Implement Pod Security standards in the Pod's YAML configuration.

D. Deploying Pods with randomly generated names to obfuscate their identities.

Answer: C

Question: 5

What was the name of the precursor to Pod Security Standards?

A. Container Runtime Security

B. Kubernetes Security Context

C. Container Security Standards

D. Pod Security Policy

Answer: D

Question: 6

Which of the following is a control for Supply Chain Risk Management according to NIST 800-53 Rev.

5?

A. Access Control

B. System and Communications Protection

C. Supply Chain Risk Management Plan

D. Incident Response

Answer: C

Question: 7

In a Kubernetes environment, what kind of Admission Controller can modify resource manifests when applied to the Kubernetes API to fix misconfigurations automatically?

A. ValidatingAdmissionController

B. PodSecurityPolicy

C. MutatingAdmissionController

D. ResourceQuota

Answer: C

Question: 8

By default, in a Kubeadm cluster, which authentication methods are enabled?

A. OIDC, Bootstrap tokens, and Service Account Tokens

B. X509 Client Certs, OIDC, and Service Account Tokens

C. X509 Client Certs, Bootstrap Tokens, and Service Account Tokens

D. X509 Client Certs, Webhook Authentication, and Service Account Tokens

Answer: C

Question: 9

A container running in a Kubernetes cluster has permission to modify host processes on the underlying node.

What combination of privileges and capabilities is most likely to have led to this privilege escalation?

A. There is no combination of privileges and capabilities that permits this.

B. hostPID and SYS_PTRACE

C. hostPath and AUDIT_WRITE

D. hostNetwork and NET_RAW

Answer: A

Question: 10

What is the purpose of the Supplier Assessments and Reviews control in the NIST 800-53 Rev. 5 set of controls for Supply Chain Risk Management?

A. To evaluate and monitor existing suppliers for adherence to security requirements.

B. To conduct regular audits of suppliers' financial performance.

C. To establish contractual agreements with suppliers.

D. To identify potential suppliers for the organization.

Answer: A

Question: 11

What mechanism can I use to block unsigned images from running in my cluster?

A. Enabling Admission Controllers to validate image signatures.

B. Using PodSecurityPolicy (PSP) to enforce image signing and validation.

C. Using Pod Security Standards (PSS) to enforce validation of signatures.

D. Configuring Container Runtime Interface (CRI) to enforce image signing and validation.

Answer: A

Question: 12

What is the main reason an organization would use a Cloud Workload Protection Platform (CWPP) solution?

A. To protect containerized workloads from known vulnerabilities and malware threats.

B. To automate the deployment and management of containerized workloads.

C. To manage networking between containerized workloads in the Kubernetes cluster.

D. To optimize resource utilization and scalability of containerized workloads.

Answer: A

Question: 13

Which other controllers are part of the kube controller manager inside the Kubernetes cluster?

A. Job controller, CronJob controller, and DaemonSet controller

B. Pod, Service, and Ingress controller

C. Namespace controller, ConfigMap controller, and Secret controller

D. Replication controller, Endpoints controller, Namespace controller, and ServiceAccounts controller

Answer: D

Question: 14

What is Grafana?

A. A cloud-native distributed tracing system for monitoring microservices architectures.

B. A container orchestration platform for managing and scaling applications.

C. A platform for monitoring and visualizing time-series data.

D. A cloud-native security tool for scanning and detecting vulnerabilities in Kubernetes clusters.

Answer: C

Question: 15

Which of the following statements best describe container image signing and verification in the cloud environment?

A. Container image signatures and their verification ensure their authenticity and integrity against tampering.

B. Container image signatures are concerned with defining developer ownership of applications within multi-tenant environments.

C. Container image signatures are mandatory in cloud environments, as cloud providers would deny the execution of unsigned container images.

D. Container image signatures affect the performance of containerized applications, as they increase the size of images with additional metadata.

Answer: A

Question: 16

Which technology can be used to apply security policy for internal cluster traffic at the application layer of the network?

A. Network Policy

B. Ingress Controller

C. Container Runtime

D. Service Mesh

Answer: D

Question: 17

In the event that kube-proxy is in a CrashLoopBackOff state, what impact does it have on the Pods running on the same worker node?

A. The Pods cannot communicate with other Pods in the cluster.

B. The Pod cannot mount persistent volumes through CSI drivers.

C. The Pod's security context restrictions cannot be enforced.

D. The Pod's resource utilization increases significantly.

Answer: A

Question: 18

Which label should be added to the Namespace to block any privileged Pods from being created in that Namespace?

A. privileged: false

B. privileged: true

C. pod-security.kubernetes.io/enforce: baseline

D. pod.security.kubernetes.io/privileged: false

Answer: C

Question: 19

Which way of defining security policy brings consistency, minimizes toil, and reduces the probability of misconfiguration?

A. Using a declarative approach to define security policies as code.

B. Relying on manual audits and inspections for security policy enforcement.

C. Manually configuring security controls for each individual resource, regularly.

D. Implementing security policies through manual scripting on an ad-hoc basis.

Answer: A

Question: 20

What kind of organization would need to be compliant with PCI DSS?

A. Retail stores that only accept cash payments.

B. Government agencies that collect personally identifiable information.

C. Non-profit organizations that handle sensitive customer data.

D. Merchants that process credit card payments.

Answer: D

Question: 21

What is the reasoning behind considering the Cloud as the trusted computing base of a Kubernetes cluster?

A. The Cloud enforces security controls at the Kubernetes cluster level, so application developers can focus on applications only.

B. A Kubernetes cluster can only be trusted if the underlying Cloud provider is certified against international standards.

C. A vulnerability in the Cloud layer has a negligible impact on containers due to Linux isolation mechanisms.

D. A Kubernetes cluster can only be as secure as the security posture of its Cloud hosting.

Answer: D

Question: 22

A cluster is failing to pull more recent versions of images from k8s.gcr.io. Why may this be?

A. There is a network connectivity issue between the cluster and k8s.gcr.io.

B. There is a bug in the container runtime or the image pull process.

C. The authentication credentials for accessing k8s.gcr.io are incorrectly scoped.

D. The container image registry k8s.gcr.io has been deprecated.

Answer: D

Question: 23

Which information does a user need to verify a signed container image?

A. The image's SHA-256 hash and the private key of the signing authority.

B. The image's digital signature and the private key of the signing authority.

C. The image's SHA-256 hash and the public key of the signing authority.

D. The image's digital signature and the public key of the signing authority.

Answer: D

Question: 24

In order to reduce the attack surface of the Scheduler, which default parameter should be set to false?

A. --scheduler-name

B. --profiling

C. --secure-kubeconfig

D. --bind-address

Answer: B

Question: 25

Which of the following statements correctly describes a container breakout?

A. A container breakout is the process of escaping the container and gaining access to the Pod's network traffic.

B. A container breakout is the process of escaping a container when it reaches its resource limits.

C. A container breakout is the process of escaping the container and gaining access to the cloud provider's infrastructure.

D. A container breakout is the process of escaping the container and gaining access to the host operating system.

Answer: D

Question: 26

When using a cloud provider's managed Kubernetes service, who is responsible for maintaining the etcd cluster?

A. Kubernetes administrator

B. Namespace administrator

C. Cloud provider

D. Application developer

Answer: C

Question: 27

What is the purpose of an egress NetworkPolicy?

A. To control the incoming network traffic to a Kubernetes cluster.

B. To control the outbound network traffic from a Kubernetes cluster.

C. To secure the Kubernetes cluster against unauthorized access.

D. To control the outgoing network traffic from one or more Kubernetes Pods.

Answer: D

Question: 28

What information is stored in etcd?

A. Etcd manages the configuration data, state data, and metadata for Kubernetes.

B. Application logs and monitoring data for auditing and troubleshooting purposes.

C. Sensitive user data such as usernames and passwords.

D. Pod data contained in Persistent Volume Claims (e.g. hostPath).

Answer: A

Question: 29

On a client machine, what directory (by default) contains sensitive credential information?

A. /etc/kubernetes/

B. $HOME/.kube

C. /opt/kubernetes/secrets/

D. $HOME/.config/kubernetes/

Answer: B

Question: 30

A user runs a command with kubectl to apply a change to a deployment. What is the first Kubernetes component that the request reaches?

A. Kubernetes Controller Manager

B. Kubernetes API Server

C. Kubernetes Scheduler

D. kubelet

Answer: B

Question: 31

When should soft multitenancy be used over hard multitenancy?

A. When the priority is enabling resource sharing and efficiency between tenants.

B. When the priority is enabling complete isolation between tenants.

C. When the priority is enabling fine-grained control over tenant resources.

D. When the priority is enabling strict security boundaries between tenants.

Answer: A

Question: 32

Which of the following represents a baseline security measure for containers?

A. Implementing access control to restrict container access.

B. Configuring a static IP for each container.

C. Configuring persistent storage for containers.

D. Run containers as the root user.

Answer: A

Question: 33

How do Kubernetes namespaces impact the application of policies when using Pod Security Admission?

A. Namespaces are ignored; Pod Security Admission policies apply cluster-wide only.

B. Different policies can be applied to specific namespaces.

C. Each namespace can have only one active policy.

D. The default namespace enforces the strictest security policies by default.

Answer: B

Question: 34

Which of the following statements on static Pods is true?

A. The kubelet can run static Pods that span multiple nodes, provided that it has the necessary privileges from the API server.

B. The kubelet can run a maximum of 5 static Pods on each node.

C. The kubelet schedules static Pods local to its node without going through the kube-scheduler, making tracking and managing them difficult.

D. The kubelet only deploys static Pods when the kube-scheduler is unresponsive.

Answer: C

Question: 35

Which of the following is a valid security risk caused by having no egress controls in a Kubernetes cluster?

A. Denial of Service

B. Data exfiltration

C. Increased attack surface

D. Unauthorized access to external resources

Answer: B

Question: 36

An attacker has access to the network segment that the cluster is on.

What happens when a compromised Pod attempts to connect to the API server?

A. The compromised Pod is automatically isolated from the network to prevent any connections to the API server.

B. The compromised Pod is allowed to connect to the API server without any restrictions.

C. The compromised Pod attempts to connect to the API server, but its requests may be blocked due to network policies.

D. The compromised Pod connects to the API server and is granted elevated privileges by default.

Answer: C

Question: 37

What is a multi-stage build?

A. A build process that involves multiple developers collaborating on building an image.

B. A build process that involves multiple repositories for storing container images.

C. A build process that involves multiple containers running simultaneously to speed up the image creation.

D. A build process that involves multiple stages of image creation, allowing for smaller, optimized images.

Answer: D

Question: 38

Is it possible to restrict permissions so that a controller can only change the image of a deployment (without changing anything else about it, e.g., environment variables, commands, replicas, secrets)?

A. Yes, by granting permission to the /image subresource.

B. Not with RBAC, but it is possible with an admission webhook.

C. No, because granting access to the spec.containers.image field always grants access to the rest of the spec object.

D. Yes, with a 'managed fields' annotation.

Answer: A

Question: 39

Which of the following statements best describes the role of the Scheduler in Kubernetes?

A. The Scheduler is responsible for monitoring and managing the health of the Kubernetes cluster.

B. The Scheduler is responsible for ensuring the security of the Kubernetes cluster and its components.

C. The Scheduler is responsible for managing the deployment and scaling of applications in the Kubernetes cluster.

D. The Scheduler is responsible for assigning Pods to nodes based on resource availability and other constraints.

Answer: D

Question: 40

An attacker has successfully overwhelmed the Kubernetes API server in a cluster with a single control plane node by flooding it with requests.

How would implementing a high-availability mode with multiple control plane nodes mitigate this attack?

A. By implementing network segmentation to isolate the API server from the rest of the cluster, preventing the attack from spreading.

B. By distributing the workload across multiple API servers, reducing the load on each server.

C. By increasing the resources allocated to the API server, allowing it to handle a higher volume of requests.

D. By implementing rate limiting and throttling mechanisms on the API server to restrict the number of requests allowed.

Answer: B

Question: 41

Which of the following snippets from a RoleBinding correctly associates user bob with Role podreader ?

O iiA)Kti:
- kind* Uwr flaw pod roodor ApiGroup rWc .Author Hath*, kit-io rolaRafr kind Role "onr boh Api Group: rboc .AuthorHot)o#i.kf«. jo

0 *ub}xt« kindr U«or naw- bob *piGroup: rbx. luthorj^itiM.kt*. io roUlUfi
kind Me
AA*O- pod ■r»«d»r
«plO«M>: rUc.MthsHiCtiMi.Ui.iO

0 #*!•«*:
* kind: Ui«r mw: bob jplOoup: rtac.MthOrUMlon.Ut. Io
rolAROi.
kind: ClwiftrRolo M«Ai fxxjr radar *P I Group: rbof Author|ratiao.bli^jQ

O wbjecti:
kind: Group flow bob ApjGruup: rhaf.Authoriiation.UR*.ip
roloUf: kind: Hole no«o pad-rrador opiGroup: rbot Author i Mt ion. MH 3 o

A. Option A

B. Option B

C. Option C

D. Option D

Answer: B

Question: 42

A container image is trojanised by an attacker by compromising the build server. Based on the STRIDE threat modeling framework, which threat category best defines this threat?

A. Repudiation

B. Spoofing

C. Denial of Service

D. Tampering

Answer: D

Question: 43

You are responsible for securing the kubelet component in a Kubernetes cluster.

Which of the following statements about kubelet security is correct?

A. Kubelet runs as a privileged container by default.

B. Kubelet does not have any built-in security features.

C. Kubelet supports TLS authentication and encryption for secure communication with the API server.

D. Kubelet requires root access to interact with the host system.

Answer: C

Question: 44

Which step would give an attacker a foothold in a cluster but no long-term persistence?

A. Modify Kubernetes objects stored within etcd.

B. Modify file on host filesystem.

C. Starting a process in a running container.

D. Create restarting container on host using Docker.

Answer: C

Question: 45

In a cluster that contains Nodes with multiple container runtimes installed, how can a Pod be configured to be created on a specific runtime?

A. By using a command-line flag when creating the Pod.

B. By modifying the Docker daemon configuration.

C. By setting the container runtime as an environment variable in the Pod.

D. By specifying the container runtime in the Pod's YAML file.

Answer: D

Question: 46

Why does the default base64 encoding that Kubernetes applies to the contents of Secret resources provide inadequate protection?

A. Base64 encoding is vulnerable to brute-force attacks.

B. Base64 encoding relies on a shared key which can be easily compromised.

C. Base64 encoding does not encrypt the contents of the Secret, only obfuscates it.

D. Base64 encoding is not supported by all Secret Stores.

Answer: C

Question: 47

Why might NetworkPolicy resources have no effect in a Kubernetes cluster?

A. NetworkPolicy resources are only enforced if the Kubernetes scheduler supports them.

B. NetworkPolicy resources are only enforced if the networking plugin supports them.

C. NetworkPolicy resources are only enforced for unprivileged Pods.

D. NetworkPolicy resources are only enforced if the user has the right RBAC permissions.

Answer: B

Question: 48

Which security knowledge-base focuses specifically on offensive tools, techniques, and procedures?

A. MITRE ATT&CK

B. OWASP Top 10

C. CIS Controls

D. NIST Cybersecurity Framework

Answer: A

Question: 49

What does the 'cluster-admin' ClusterRole enable when used in a RoleBinding?

A. It gives full control over every resource in the role binding's namespace, not including the namespace object for isolation purposes.

B. It gives full control over every resource in the cluster and in all namespaces.

C. It gives full control over every resource in the role binding's namespace, including the namespace itself.

D. It allows read/write access to most resources in the role binding's namespace. This role does not allow write access to resource quota, to the namespace itself, and to EndpointSlices (or Endpoints).

Answer: B

Question: 50

Which of the following statements regarding a container run with privileged: true is correct?

A. A container run with privileged: true within a cluster can access all Secrets used within that cluster.

B. A container run with privileged: true within a Namespace can access all Secrets used within that Namespace.

C. A container run with privileged: true on a node can access all Secrets used on that node.

D. A container run with privileged: true has no additional access to Secrets than if it were run with privileged: false.

Answer: D

Question: 51

A Kubernetes cluster tenant can launch privileged pods in contravention of the restricted Pod Security Standard mandated for cluster tenants and enforced by the built-in PodSecurity admission controller.

The tenant has full CRUD permissions on the namespace object and the namespaced resources. How did the tenant achieve this?

A. The scope of the tenant role means privilege escalation is impossible.

B. By tampering with the namespace labels.

C. By deleting the PodSecurity admission controller deployment running in their namespace.

D. By using higher-level access credentials obtained reading secrets from another namespace.

Answer: B

Question: 52

In Kubernetes, what is Public Key Infrastructure used for?

A. To manage certificates and ensure secure communication in a Kubernetes cluster.

B. To automate the scaling of containers in a Kubernetes cluster.

C. To manage networking in a Kubernetes cluster.

D. To monitor and analyze performance metrics of a Kubernetes cluster.

Answer: A

Question: 53

As a Kubernetes and Cloud Native Security Associate, a user can set up audit logging in a cluster. What is the risk of logging every event at the full RequestResponse level?

A. No risk, as it provides the most comprehensive audit trail.

B. Increased storage requirements and potential impact on performance.

C. Improved security and easier incident investigation.

D. Reduced storage requirements and faster performance.

Answer: B

Question: 54

Given a standard Kubernetes cluster architecture comprising a single control plane node (hosting both etcd and the control plane as Pods) and three worker nodes, which of the following data flows crosses a trust boundary?

A. From kubelet to Container Runtime

B. From kubelet to API Server

C. From kubelet to Controller Manager

D. From API Server to Container Runtime

Answer: B

Question: 55

To restrict the kubelet's rights to the Kubernetes API, what authorization mode should be set on the Kubernetes API server?

A. Node

B. AlwaysAllow

C. kubelet

D. Webhook

Answer: A

Question: 56

Which of the following statements is true concerning the use of microVMs over user-space kernel implementations for advanced container sandboxing?

A. MicroVMs allow for easier container management and orchestration than user-space kernel implementation.

B. MicroVMs offer higher isolation than user-space kernel implementations at the cost of a higher per-instance memory footprint.

C. MicroVMs provide reduced application compatibility and higher per-system call overhead than user-space kernel implementations.

D. MicroVMs offer lower isolation and security compared to user-space kernel implementations.

Answer: B

Question: 57

In which order are the validating and mutating admission controllers run while the Kubernetes API server processes a request?

A. The order of execution varies and is determined by the cluster configuration.

B. Validating admission controllers run before mutating admission controllers.

C. Validating and mutating admission controllers run simultaneously.

D. Mutating admission controllers run before validating admission controllers.

Answer: D

Question: 58

A cluster administrator wants to enforce the use of a different container runtime depending on the application a workload belongs to.

A. By manually modifying the container runtime for each workload after it has been created.

B. By modifying the kube-apiserver configuration file to specify the desired container runtime for each application.

C. By configuring a validating admission controller webhook that verifies the container runtime based on the application label and rejects requests that do not comply.

D. By configuring a mutating admission controller webhook that intercepts new workload creation requests and modifies the container runtime based on the application label.

Answer: C

Question: 59

How can a user enforce the Pod Security Standard without third-party tools?

A. Through implementing Kyverno or OPA Policies.

B. Use the PodSecurity admission controller.

C. It is only possible to enforce the Pod Security Standard with additional tools within the cloud native ecosystem.

D. No additional measures have to be taken to enforce the Pod Security Standard.

Answer: B