INFOSECTRAIN

Cloud Security Engineer

Interview Questions

https://www.infosectrain.com sales@infosectrain.com

Introduction

With the expanding demands of business and the changing IT landscape, more and more companies are shifting to cloud technology. Cloud security is a significant issue among businesses considering a shift to the cloud, as new threats emerge on a daily basis. Due to this, there is a demand for professionals who can address the security concerns present in the realm of cloud computing and help mitigate them.

Cloud Security Engineers play a crucial role in ensuring the cloud's security posture. Therefore, there is a massive demand for these individuals, who are compensated well. So, we have compiled the latest Cloud Security Engineer interview questions and answers to help you prepare for your interview so you can ace it in the first go.

Question 1: What is cloud security?

Answer: Cloud security is the application of cutting-edge technologies, methodologies, and programming to protect your cloud-hosted data, applications, and services, as well as the infrastructure that supports them.

Question 2: What security precautions are needed before transferring to the cloud?

Answer: Some of the security measures are:

• You must be familiar with the shared responsibility model because cloud providers operate under it. You must be aware of what your cloud provider will provide and what you will be accountable for in terms of security in the cloud.

• Centralize your monitoring for threats and vulnerabilities since cloud connectivity might indicate an increase in the potential for attacks and an increase in speed and number.

• Encryption of data.

• When migrating to the cloud, it is essential to understand what, if any, regulatory and compliance standards apply to your data.

Question 3: What technologies are employed to ensure that cloud computing is secure and that the enterprise's data is safeguarded?

Answer: Some of them are:

• Use a cloud provider who can provide proper encryption technologies for your files in the cloud and your device.

• Use strong passwords and update them frequently, as well as do not use the same password for many accounts.

• Do not share your personal information

• Avoid storing confidential data in the cloud.

• Have powerful antivirus and anti-malware security on your devices because the cloud transmits data over the internet.

• Configure your privacy settings as soon as you sign up for a cloud service provider to ensure that you are not disclosing your private information through the apps you connect to your service provider.

• Assure that your operating system is up to date.

Question 4: What security features does the cloud offer?

Answer: The following are the five aspects of cloud security:

1. SECURE ARCHITECTURE
2. ENFORCING COMPLIANCE
3. MONITORING THE NETWORK
4. PRACTICING DUE DILIGENCE
5. INCORPORATING STRONG AUTHENTICATION PROTOCOL

Question 5: Are you familiar with the Windows Azure operating system?

Answer: Windows Azure is a virtualized environment that runs on a Hyper-V platform that has been customized. The host OS is in charge of managing the server's resources as well as executing the Windows Azure Agent, which communicates with the Windows Azure Fabric Controller. Windows Azure isn't a single OS but rather a collection of several OSs that function together.

Question 6: What are the security laws to protect data in the cloud?

Answer: The security laws are:

• **Input validation:** This essentially regulates the data fed into any system.

• **Output reconciliation:** Keeping track of data that must be reconciled from input to output.

• **Processing:** This refers to the assurance that data is correctly and completely processed within an application.

• **File:** Managing the data that is placed in any file.

• **Backup and recovery:** Manages the security breaches and resolves issues that arise when creating backups and recovery.

Question 7: Explain cloud security architecture?

Answer: A cloud security architecture comprises the security layers, design, and structure of the platform, software, tools, infrastructure, and best practices that exist within a cloud environment.

Question 8: What are the many layers that make up the cloud architecture?

Answer: The various layers in cloud architecture are:

- Physical server
- Computing resources
- Storage resources
- Hypervisor
- Virtual Machine (VM)

Question 9: What are the different phases of cloud architecture?

Answer: The various phases involved in cloud architecture are:

- Launch phase
- Monitor phase
- Shutdown phase
- Cleanup phase

Question 10: How do you keep Kubernetes clusters safe?

Answer: Some of the measures to secure Kubernetes clusters safe are:

• You should enable the Role-Based Access Control (RBAC) in Kubernetes.

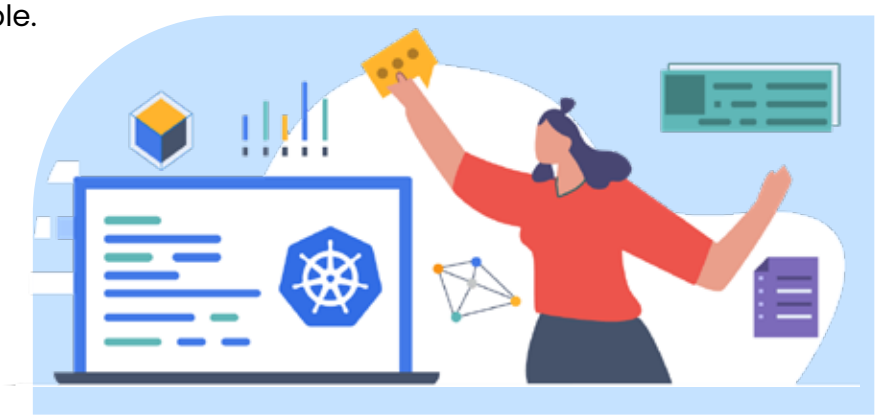
• TLS, Firewall, and Encryption should all be used to secure etcd.

• Kubernetes nodes must be on their private network and not be connected to the internet.

• Always use the most recent version of Kubernetes and upgrade your Kubernetes version to the most current version available.

• Aqua should be used to secure Kubernetes.

• For API servers, you should use third-party authentication.



Question 11: What is Eucalyptus in cloud computing?

Answer: Eucalyptus or Elastic Utility Computing Architecture for Linking Your Programs to Useful Systems is an open-source software framework that serves as a foundation for implementing private cloud computing on computer clusters. For web services, it is built with an extensible and modular architecture.

Question 12: What is the purpose of a PodSecurityPolicy?

Answer: A PodSecurityPolicy is a resource you define in the admission controller that validates requests to create and edit Pods in your cluster. It is used to describe a Pod's security policies, such as whether it should run as root or not.

Question 13: What is an Amazon Web Services (AWS) placement group?

Answer: Placement groups are a logical way of arranging interdependent instances in a specific area. A placement group is a collection of AWS instances that share the same availability zone when members of a group are able to communicate with one another with low latency and high throughput.

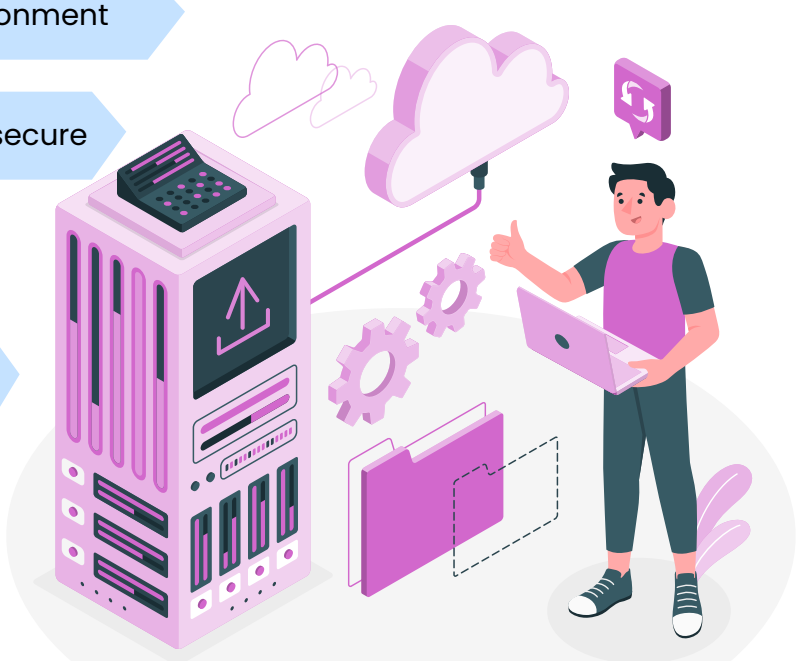
Question 14: What is the CIA, and why is it important?

Answer: The CIA triad refers to Confidentiality, Integrity, and Availability. It is a concept for guiding information security policy inside an organization. It is significant in cybersecurity because it provides critical security features, aids in the avoidance of compliance concerns, maintains business continuity, and protects the organization's reputation.

Question 15: What security measures would you take in a containerized environment?

Answer: The following are the steps to secure containerized environments:

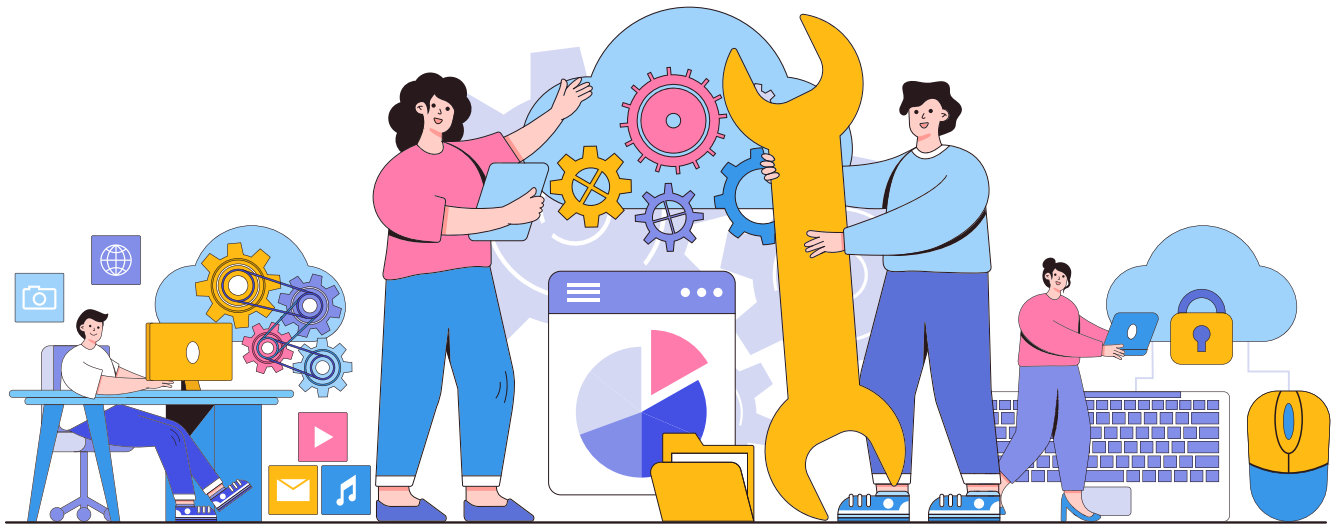
- Keep the container host secure
- Maintain a secure networking environment
- Ensure your management stack is secure
- Create a solid foundation
- Ensure your build pipeline is safe
- Ensure your app is secure



Question 16: How would you protect a distinct workload in the cloud?

Answer: A cloud workload is a specific capacity or task that we assign to a cloud instance. Some of the measures to secure distinct cloud workloads are:

- Management of vulnerabilities and configurations, including patching
- Monitoring and managing the security of your network
- When using IaaS, encrypting data at rest and in transit is essential
- Antivirus software installation
- Defending the memory and preventing exploits
- Using advanced behavioral response and detection techniques



Question 17: Explain the security architecture of the IaaS cloud service model.

Answer: IaaS is a cloud service that provides necessary computation, storage, and networking capabilities on demand. The organizations get the infrastructure from a cloud provider, and companies install their own operating systems, applications, and middleware because the systems and networks can be set up instantaneously.

The security risks for IaaS are the same as those for on-premise systems. Therefore, standard security tools and cloud-specific solutions, such as CASBs, Endpoint Protection (EPP), vulnerability management, IAM, and data encryption, should all be in place. Using these in conjunction with one another generates layers of security, resulting in a more effective security plan.

Question 18: Explain the security architecture of the PaaS cloud service model.

Answer: PaaS is a cloud-based development and deployment environment with resources to help you deliver applications. It is essentially a place where businesses can buy a platform from a cloud provider that enables the organization to design, maintain, and manage apps without worrying about the underlying infrastructure traditionally necessary to execute them.

In general, security vulnerabilities in PaaS are self-inflicted, such as misconfiguration and unauthorized access, which result in application security being compromised. As a result, securing your PaaS environment necessitates the use of both standard cloud security and non-standard security solutions. That means CSP safeguards the majority of the environment in PaaS. However, the corporation is still responsible for the protection of the applications it creates.

Question 19: Explain the security architecture of the SaaS cloud service model.

Answer: SaaS allows you to use apps that you may buy online from a cloud provider or a corporation hosted in the cloud, such as Dropbox, Salesforce, Gmail, and so on. With SaaS, the customer just only consumes the application and the provider usually handles the end-to-end part. Still, users are liable for compliance and data security. Users should consider using Cloud Access Security Brokers (CASB) to assist with protecting these apps by giving users visibility, access restrictions, and data protection by utilizing APIs, proxies, or gateways to thwart various security threats in SaaS such as phishing attacks or insider threats.

Question 20: Mention some databases on open source cloud computing platforms?

Answer: Some of the open-source databases are:

mongo DB

LUCID DB

CouchDB

INFOSECTRAIN

THANKS

https://www.infosectrain.com

sales@infosectrain.com