By OnlineInterviewQuestions.com

Cyber Security Interview Questions

Cyber Security is the protection of data that has been made available on the internet. It helps in the protection of the integrity of different computing properties that belong to a particular organization. The purpose of cybersecurity professionals is to defend against the multitude of threats that are available on the internet. Cybersecurity has never been easy mainly because every day there is a new threat that evolves, as attackers keep getting more and more inventive.

Losing an important piece of information or any data can put the organization in a very difficult position. Due to this, organizations are hiring individuals that have immense knowledge and experience in the field of cybersecurity. Thus, many multinational companies and even different business firms ask a variety of **cybersecurity interview questions** to not only fresh recruits but also experienced individuals wishing to display their talent and knowledge in this field. Here are some important **cybersecurity interview questions** that will not only give you a basic idea of the field but also help to clear the interview.

Practice Best Cyber Security Interview Questions

Practice best **Cyber Security Interview Questions and Answers**, for the best preparation of the CyberSecurity Interview. These **Cyber Security Interview Questions** are very popular & helpful for fresher & experienced candidates. So, practice these questions to check the final preparation for your interviews. apart from this, you can also download the **Cyber Security Interview Questions PDF**, completely free.

Q1. What is risk, vulnerability and threat?

Start by explaining vulnerability, and threat and lastly risk.

Vulnerability (weakness) is a break in the security efforts of a system whereas a threat is an intruder who misuses that vulnerability. The risk is the measure of possible loss when the threat exploits that vulnerability. You may also give an example of your own.

Q2. Differentiate between Asymmetric and Symmetric encryption.

- Asymmetric encryption utilizes different keys for encryption and decryption process. Symmetric encryption utilizes the same key for both encryption and decryption process.
- Asymmetric encryption is a slow process. Symmetric is faster and requires the key to being transferred via an unencrypted channel.

Q3. Differentiate between encryption and hashing.

Characteristics of encryption:

- It is reversible
- Ensures confidentiality

Characteristics of hashing:

- It is irreversible
- It can be cracked using rainbow tables
- Ensures integrity

Q4. Describe CSRF

CSRF is an acronym for Cross-Site Request Forgery, which is a web application vulnerability wherein the server does not verify whether the request has come from a trusted client or not. The request is processed immediately. It can be in addition accompanied by the methods to become aware of such conditions using examples and countermeasures.

Q5. What do you understand by Security Misconfiguration?

Security Misconfiguration is also a vulnerability condition like CSRF that occurs when a device, application or network is configured such a way that it can be easily exploited by an attacker. Examples of such kind of threat include keeping the sample username and password, using too simple combinations for all the devices, etc.

Q6. Describe a firewall.

A Firewall is a device, which allows or blocks off traffic as directed by a set of rules. Firewalls are generally placed at the boundaries of trusted as well as untrusted networks.

Q7. List some of the various codes from a web application.

- 1xx – information responses
- 2xx – success
- 3xx – redirection
- 4xx – client side error
- 5xx – server side error

Q8. What are the basic components of a basic web architecture?

The basic web architecture consists of the following basic components:

- front-end server
- web application server
- database server

Q9. What frequency should be maintained while performing Patch management?

Patch management should be carried out as soon as possible. For Windows operating system – patches should be released every second Tuesday of the month by Microsoft and it should be incorporated into all the machines within a duration of less than one month.

Q10. What procedure is applied to run security objects?

Different security objects are run with the assistance of Key Performance Indicators (KPI). For example in case of a Windows Patch, if the KPI agreed is 99%, it means that 99% of the computers will have the latest patch within a duration of one month of its release.

Q11. Differentiate between policies, processes and guidelines

- A security policy is a security objective and security framework of a particular organization.
- A process is a detailed description with a step by step guidelines as to how to document a specific action which needs to be importantly implemented.
- Guidelines are various recommendations that can be customized to create new procedures.

Q12. How can one manage antivirus alerts or threats?

In order to manage an antivirus alert, firstly check the policy concerning the antivirus and the alert. If the alert is genuine, it can then be whitelisted or else it is deleted or quarantined. After which the hash of the file is checked for reputation on different websites. Finally, the antivirus is fine-tuned so as to reduce the threat and protect the device.

Q13. What is a data leakage and how can it be detected and prevented?

Data leakage occurs when the data gets out the organization in an unauthorized manner. Data can be leaked in multiple ways such as emails, prints, losing laptops, the uploading of unauthorized data to different public portals, photographs, etc.

In order to detect and prevent leakage of data, various control measures can be taken. They include:

- restriction of data that is being uploaded onto the internet
- websites carrying out a thorough internal encryption solution
- placing a restriction on emails being sent on internal networks
- keeping a check on data that is being printed
- Maintain confidentiality etc.

Q14. List the different levels of data classification

Data is generally classified into the following three levels:

- Top Secret – in this level the leakage can cause an extreme consequence on the organization. For instance the leakage of trade secrets.
- Confidential – internal data that represents the organization, for examples policies and processes
- Public – these include the data that is publically available to the masses, for example, newsletters, flyers, etc.

Q15. What is the importance of data classification?

Data has to be classified into different categories so that the severity (in case of leakage) can be well defined and identified. Without proper segregation of data, the crucial piece of information cannot be classified as critical or non-critical for other members of the organization.

Q16. Describe the various methodologies adopted to ensure that employees are aware of the security policies and procedures.

Various methods adopted to ensure that employees are aware of the security policies and procedures include:

- Employees need to undergo a compulsory information security training post before joining the company. This is also done on a yearly basis.
- Distribution or sending notifications on a regular basis in different forms such as slides, pages can help ensure that employees are well aware of the security policies and procedures.

Q17. What are the components of a CEO level report from a security standpoint?

The basic components of a CEO level report include:

- A summarized page with the state of security prevailing within the organization
- Results of Annual Loss Expectancy and Quantified risk along with its countermeasures