Cybersecurity Interview Questions

1) About yourself

2) Past job experience

3) What do you know about the company?

- Values
- Mission
- Vision
- Products / Services
- Services
- Look for the company's annual report 2021/2022
- Company's predictions

4) Recent research of the company

- R&D research
- Look for hashtags mentioned by the company's executives in their LinkedIn posts
- Search for the hashtags and news on Keysight products/research
- Look for conferences/forums/interviews participated by the company's CEO and executives

5) Cybersecurity channels/websites/ podcasts that you follow

6) What is the industry of your company?

- Ex: Telecommunication / Manufacturing / Automotive and etc

7) When looking at cybersecurity what are the most prominent threats presented to the industry mentioned in no (6)?

8) What more do you think the industry could/should be doing when looking at cybersecurity threats?

9) Cybersecurity knowledge

- NIST framework
- Layers of the OSI model
- CIA
- Cyber kill chain
- MITRE Attack
- Information Security and Compliance (ISC)
- Cloud Services
- IOTs
- OT vs IT
- # Of ports 65535
- Firewall vs IPS vs IDS
- VPN
- DMZ
- TCP Three-way handshake.
- Endpoint Detection and Response (EDR)
- Common Vulnerabilities and Exposures (CVE)
- Common Vulnerability Scoring System (CVSS)
- Pentesting testing vs vulnerability assessment
- Indicator of Compromise (IOC)
- Indicators of attack (IOA)

10) What are your strength and weakness?

11) What is your #1 quality?

12) What are the latest vulnerabilities or cyber threats found?

- **ZuoRAT**
- **MedusaLocker** ransomware actors
- **Remote code execution** vulnerability (CVE-2022-26134) affecting **Confluence Server** and **Data Center** products
- **Log4Shell** is compromising public-facing **VMware Horizon** and **Unified Access Gateway (UAG) servers**.
- **Advanced persistent threat group Fancy Bear** is pushing malicious documents weaponized with the exploit for **Follina** (CVE-2022-30190) via phishing. Fancy Bear is also known as **APT28,** Strontium, and Sofacy.

13) What are the common industry (mentioned in no. 6) vulnerabilities or cyber-attacks?

14) Why this company?

15) What do you find interesting about cybersecurity?

16) Why did you choose cybersecurity to build your career?

17) Review the JD and highlights your skills related to the JD

18) Your expectations from this job & company

- Looking for mentors
- Open communication
- Development opportunities
- Healthy working environment
- Fair compensation
- Career advancement