**Security Posture & Risk Assessment**

**Interview Questions**

The following set of questions has been prepared for the purpose of this interview. Some questions may require concise, one-sentence responses, while others may call for more detailed information. Please feel free to answer to the best of your ability. If any question involves sensitive or confidential information that you are not comfortable sharing, it is entirely acceptable to refrain from providing those details. However, we kindly encourage you to share as much relevant information as possible, as your insights are greatly valued.

**1. General IT & Security Questions**

* What security frameworks does your organization follow (e.g., NIST, ISO 27001, CIS Controls)?
* How does your organization monitor and respond to security threats?
* What is the organization's approach to security awareness training?

**2. Shadow IT & Unauthorized Applications**

* How does the organization identify and track unauthorized IT resources (Shadow IT)?
* What policies are in place to regulate the use of third-party cloud applications?

**3. Network & Data Security**

* How is network traffic monitored for potential threats and anomalies?
* What security measures are in place to protect critical data (encryption, backups, access control)?
* How often are security audits and vulnerability assessments conducted?
* Are there any known vulnerabilities or security gaps in the organization's IT infrastructure?
* How is data classified based on sensitivity and protected accordingly?

**4. Incident Response & Compliance**

* What is the organization's protocol for handling security incidents?
* How quickly can the organization detect and respond to a security breach?
* How is compliance with security standards ensured and documented?

**5. Recommendations & Security Improvements**

* What are the biggest security challenges the organization currently faces?
* Are there any security enhancements planned for the near future?
* What additional security tools or practices would improve the organization's security posture?

**8. Remote Work & Mobile Device Security**

* Do employees work from home or use their phones/laptops for work?
* How do you keep remote devices safe from hackers or viruses?
* What happens if a work phone or laptop gets lost or stolen?
* Are remote workers required to use VPNs or special security tools?

**9. Software & Patch Management**

* How do you ensure all software is up to date and secure?
* How often do you review and update your software and operating systems?
* What happens if a critical patch needs to be applied quickly—how do you handle it?

**10. Firewall Configuration**

* What types of firewalls are deployed (stateful, next-gen, web application firewalls)?
* How are firewall rules audited and maintained for least privilege access?