Technical Knowledge and Skills:

Q: How do you stay updated with the latest cybersecurity threats and trends?

Q: Can you explain the difference between a virus, a worm, and a Trojan?

Q: Can you explain the difference between an alert, an event, and an incident?

Q: What is a security information and event management (SIEM) system, and how have you used it in the past?

Q: Describe the steps you would take after detecting a potential security breach.

Q: What are common indicators of compromise (IoCs), and how do you identify them?

Practical Scenarios and Problem-Solving:

Q: Describe a challenging cybersecurity problem you have solved. How did you approach it?

Q: How would you handle a situation where you detect a false positive security threat?

Q: How do you conduct a root cause analysis?

Q: What are the 5 “Whys”?

Q: What steps would you take if you discovered a new and unknown type of malware in the network?

Q: What security measures and best practices do you implement to ensure the security of remote systems and data?

Q: How do you manage user accounts and access control remotely, and what tools do you use for this purpose?

Q: Can you explain your disaster recovery and backup procedures for remote systems and data?

Q: What steps do you take to optimize the performance of remote systems and networks?

Q: How Do You Prioritize Your Work?

Communication and Teamwork:

Q: How do you communicate technical security information to non-technical staff?

Q: How do you prioritize your tasks in a high-pressure environment?

Q: How do you collaborate with a remote team, share knowledge, and document processes and configurations?

Q: How Do You Handle Stress and Pressure?

Continuous Learning and Development:

Q: What are your strategies for continuous learning and staying current in the field of cybersecurity?

Q: What strategies do you use to maintain and update systems in a remote work environment?

Q: Can you describe your experience with different operating systems, including Windows, Linux, and MacOS?

Q: Have you worked with virtualization technologies like VMware or Hyper-V in a remote setting?

Q: Can you explain your experience with remote system administration and your familiarity with remote access tools and protocols?

Q: What scripting or automation languages are you proficient in, and how do you utilize them in remote system administration?

Q: Have you worked with cloud services like AWS, Azure, or Google Cloud? If so, please elaborate on your experience.

Q: Can you discuss your experience with configuration management tools, such as Puppet or Ansible, in a remote context?

Personal:

Q: Tell Me About Yourself.

Q: What Are Your Greatest Strengths and Weaknesses?

Q: What type of position/role are you looking for?

Q: Are you comfortable working remotely, or from home?

Q: Tell me more about your home office set up?

Q: Tell me about your home lab.

Q: Are you open to a hybrid or in office role?

Q: Are there any cybersecurity certifications you currently hold or are working towards?

Q: If you could be a color, what color would you be?

Q: If you could be an animal, what animal would you be?

Q: If aliens landed on the planet in front of you and offered you any position on their planet, what would you want?

Q: If someone wrote a biography about your life, what would the title be?

Q: Sing a song that describes you.

Q: Where Do You See Yourself in Five Years?

Q: Are you willing to take a pre-employment drug test?

Q: Can you obtain a security clearance?

Q: Do you have an updated copy of your resume?