

eBook

Cybersecurity interview questions

To ask your next
Cybersecurity hire

General interviewing principles

In this Ebook you're going to find a lot of questions.

First, an overview of some of our favourite questions to ask security candidates and secondly, a deep dive into questions and scenarios for both junior and mid-level candidates.

But before we dive into that, I wanted to take a moment to go through some basic interviewing principles that can be applied to most interviews:

- Humans are bad at interviewing because we are full of biases. You're bad at it. I'm bad at it. Everyone's bad at it. And the more you know this—and work to guard against it—the better (or at least less bad) you'll be.
- The goal of interviewing should be to extract the best from the candidate, not to trick them, make them uncomfortable, or otherwise keep them from shining.
- Maintain a mentality of matching, not of filtering. Imagine that both you and the candidate are both amazing, and the only thing you're doing is seeing if you are good fit for each other.





Best security interview questions

These questions are some of the best to ask any candidate, regardless of seniority and they create a good interview flow based off a bit of experience on someones CV.

1. Tell me about a project you worked on in the past that you really enjoyed.
2. What was challenging about it?
3. Why did you choose to approach it the way you did vs. (list alternatives)
4. If you could have the perfect job and the perfect manager, what would that look like? What you do day to day, and what kind of projects would you have?
5. What is a skill you wish you had but don't yet have?
6. How are you working to get that skill?
7. What do you think the most important technology is right now?
8. How are we going to secure it?

Junior cybersecurity technical questions

These questions will help you assess a more junior cybersecurity professional and make sure they know their stuff.

What's the difference between threat, vulnerability and risk?

Answering this question calls for a deep understanding of cybersecurity and anyone working in the field should be able to give a strong response. You should expect a follow-up question asking which of the three to focus more on. Bonus points for candidates who can bring in working examples either from past experience or hypothetical.

Explain the difference between process, guidelines, and policies.

A question like this can reveal how the interviewee feels about the position and what they think they would bring to it. Some people may focus on IT certifications and technical abilities, while others may talk more about problem-solving, attention to detail, communication and other general job skills. Look for candidates who give a nice balance of both.

What does your home network look like?

Good answers here are anything that shows you the person is a computer/technology/security enthusiast and not just someone looking for a paycheck. So if she's got multiple systems running multiple operating systems you're probably in good shape.



Junior cybersecurity scenarios

This is the good stuff - these scenarios are a great way to get a candidate generating a discussion that will hopefully showcase their impressive knowledge and softskills.



A new hire has joined the company, they're using a personal device - what do you need to do to secure them?

You're just looking for the basics and the broad brush strokes of personal security.

If you were to start as a cso at a fortune 500 company with no security strategy - what would your priorities be?

We don't need a list here; we're looking for the basics. Where is the important data? Who interacts with it? Network diagrams. Visibility touch points. Ingress and egress filtering. Previous vulnerability assessments. What's being logged and audited? Etc. The key is to see that they could quickly prioritize, in just a few seconds, what would be the most important things to learn in an unknown situation.

If you had to both encrypt and compress data during transmission, which would you do first, and why?

If they don't know the answer immediately it's ok. The key is how they react. Do they panic, or do they enjoy the challenge and think through it?

Mid-level technical questions

These questions will help illustrate how your potential technical hire might work within your own team and culture.

Describe the last program or script that you wrote. What problem did it solve?

All we want to see here is if the color drains from the person's face. If they panic then we not only know they're not a programmer (not necessarily bad), but that he's afraid of programming (bad). I know it's controversial, but I think that any high-level security person needs at least some programming skills. They don't need to be a God at it, but they need to understand the concepts and at least be able to muddle through some scripting when required.

What do you look for in your projects?

You want to understand what makes the potential new candidate tick, what gets them up out of bed in the morning. Knowing this will help you build a picture of what that potential hire will look like in your current project pipeline.



Mid-level cybersecurity scenarios

How well can a candidate articulate their career milestones, and more importantly, how well can they explain the impact of these achievements?



How would you measure how well a security team is doing?

Here we're looking for them to ask us questions in return, such as, "What kind of team?" Answers that are bad include anything purely number-based like number of IDS events, or widget-thingies detected. We want to know how much experience they have tracking the things that matter vs. the things that don't.

Your security team has a new junior member and you've decided to mentor them - what do you do?

In addition to being a great communicator and being quick to learn new skills, we need to find someone who lifts others and shares their knowledge. They don't need to break out the mentorship rule book, we're just looking for the broad brushstrokes on how they would help mentor a junior member of the team.

What future technological innovations do you believe will have an impact on your job?

This question is a good way to start a conversation about trends and advancements in the field, and it will also give you insight into how the candidate perceives their role over the long term. It will also reveal a candidate's acumen for self-development.



Consultant Name

Contact Details here

evolution