Twitter Thread by Taz Wake



Taz Wake
@tazwake

So #infosec #jobs thread.
In the last 12 months, I've been involved with 60+ interviews for various SOC, IR etc roles. This has come from about 120+ CV/Resume submissions.
To start, a caveat though - this is all IMHO. Hiring is an amazingly individual event.

First CV length. The common wisdom is that it has to be under 2 pages and very tailored to the role. I disagree. A CV should be concise but it also needs to provide enough information to make the hiring manager want to speak to you. If there is an HR screen, it needs to contain

a tonne of possibly random keywords. If a job advert asks for 10 different skills, and you can fit this in to 1-2 pages, chances are the person reading it will find it missing detail and think it is unconvincing. If it's your first job a 1 page CV is ok but the more you've done

the longer your CV gets. I don't have a perfect answer but I'd say don't fret about it. A large part of the hiring process is automated and even the people who read it will read it online scrolling through to get to the bits they are interested in. Long CVs rarely put people off.

Sidenote: if they do, they are likely to be difficult to work with so you might be OK with them rejecting you after all.

Next point - and it is sad this needs to be said, but DO NOT LIE. I get that we've been told for decades to "puff" out our abilities and "fake it until you make it" but nothing kills your hiring progress faster than being caught in a lie.

Sadly about 20% of the interviews I've been part of have ended with a candidate being caught in an awkward lie, almost always un-necessary ones as well. All it does is waste everyone's time.

Common examples are claims to have certifications which they dont (if nothing else it shows ignorance about what certs can be looked up...) and claims to have skills which they dont. I've sat in interviews with people who sent CVs saying "extensive experience in disk forensics"

Then, when asked, cant say what they do or what tools they use.

With this, I dont mean asshole questions like "tell me every forensic suite" or weird ones like "whats the difference between dd and dcfldd" I mean "tell me how you would do X" type questions.

If you say "I have 5 years experience in reverse engineering malware" but can't talk to someone about what your general approach is, it creates the strong impression you have exaggerated your background.

That's enough on the candidates. They have a hard enough job as it is so it's impressive that there are very few consistent problems. However, the companies doing the hiring are often nightmares.

It seems normal for medium-large orgs to have HR and a recruitment agency involved in the hiring process. This causes all kinds of problems, but lots of hiring managers who *do the job* make life harder as well.

The biggest issue is making sure the job description is valid and useful. I've seen countless JDs which bear no relation to what the hiring manager really wants, so every candidate gets rejected. If you want someone who knows EnCase say so. If you don't, DON'T ASK FOR ENCASE.

I know that sounds simple, but it's amazing how often organisations get this wrong. I've seen one place which was a full FTK shop use a job advert which never once mentions FTK, but asks for EnCase experience. Then they complained that almost no candidates had FTK experience...

Be realistic. If you want someone with X, you need to pay for it. If you want a junior then don't expect them to know everything. If you want someone who knows packets in-depth, can script, analyse disks, carve memory etc., you are asking for someone who is VERY expensive.

The WORST mistake I see hiring managers make is to demand the people they hire know as much as they do. There is an exception but generally, this is really flawed. If they know as much or more, why would they work for you on less?

The exception is hiring a specialist. You may need someone who is a ninja in (say) Malware analysis and I wouldn't expect the manager to know more about it. However, don't expect the Malware person to talk to you about weird DNS exfil techniques. (I've actually seen that).

The last point is that interviews shouldn't be adversarial and really shouldn't turn into a certification exam. You are trying to understand what the candidate knows and if they will fit into your organisation. You should be trying to get them to explain how their experience

solves problems in your org. Sadly about 75% of interviews I've seen have had at least one interviewer basically showing off their own knowledge to the candidate. This makes no sense and often leaves the candidate feeling they are inadequate. This is not your goal.

Tl;dr

Hirers: Make your job descriptions more accurate and honest. Interview people fairly. Have realistic expectations based on what you will pay.

Candidates: Never lie. Never lie. Never lie. Stop lying.