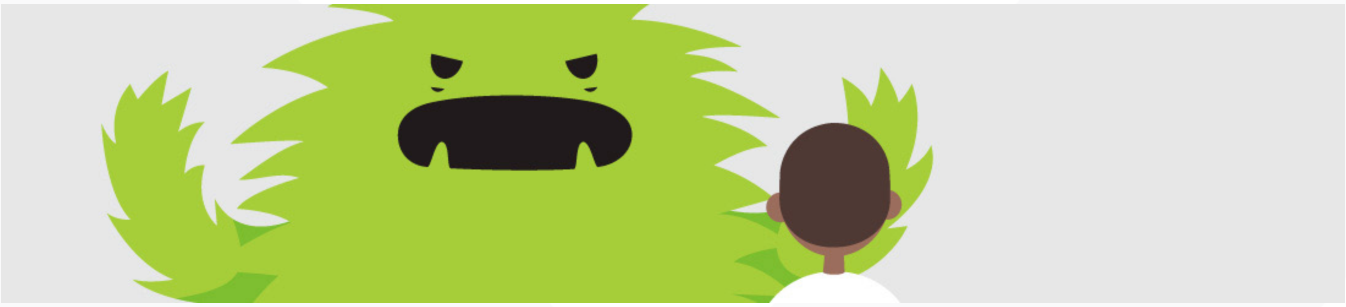

Oct 25, 2017 | Yanek Korff

Recruit for team dauntless

I was interviewing a not-very-experienced candidate recently. She'd had a number of internships in a variety of technical disciplines, but this was her first full-time role. As I do with many entry-level candidates, I asked what's known as the "what happens when..." question:

Question 1

> Imagine you're at your computer, you type "www.expel.io" into your web browser and hit enter. Tell me, in as much technical detail as you can, what happens next for that page to load.

It's a great assessment question. It's relatively hard to study for because, as an interviewer, you can keep asking more detailed questions to see where a candidate's technical depth bottoms out. The candidate can't really fully prepare for all the directions this conversation can go. This isn't a game of stump-the-candidate, but instead a way for an interviewer to assess both the breadth and depth of a candidate's technical knowledge in this area.

Our candidate did okay. Her fluency jumping around the OSI reference model implied a pretty good understanding of the network encapsulation and decapsulation process. She hit a lot of the right keywords with respect to HTTP and DNS at layer 7. She covered the handshake aspects of TCP. She even drilled down a bit into layer 2 and was able to articulate how to effectively manage a collision domain.

Where things went a little bit sideways was around DNS itself. Whether it was nerves or otherwise, she seemed to struggle separating what was happening in the routing of DNS requests from the contents of those requests and the records that would need to be returned to the DNS queries sent.

Overall, the candidate did well given her experience. She demonstrated a sufficient depth of knowledge that implied she'd be able to learn what comes next. After all, without a strong technical foundation, you can't "learn security." Your knowledge of how things work at a fundamental level forms a sort of backbone or framework onto which you can attach new things you learn. What's more, the volume of new things you learn every day in a security role is so high, it's essential to find people who have a genuine thirst for this knowledge. Some might say candidates have to be really passionate about it.

Question 2

> Tell me about a time at work, or a project at school that… thinking back to it, you say to yourself, “If I could do that every day… it was so much fun, that would be amazing.” What was this work or project? What made it so great?

Turns out, in her most recent internship, our candidate ended up solving a problem that users were having with attachments in Office 365. The process of individually downloading attachments was so cumbersome, people had written their own macros that would automatically download attachments directly to their desktop. Needless to say, the security team wasn’t excited about the proliferation of homegrown macros combined with auto-downloads.

So, the candidate dove into this problem and built a centralized capability using PowerShell and .NET that provided a safe means of retrieving, scanning, and depositing these attachments in a company-managed file share that met both the security team’s needs and the needs of their user base. Nice work!

What’s most interesting is the reason this was her favorite work experience. It’s multi-faceted. Not only did she enjoy solving a real problem that impacted users, she’d never worked with PowerShell or .NET before. Nor had she written anything to interact with Office 365. All in all, it was a tremendous learning experience. Deriving so much pleasure (remember, this was her FAVORITE work experience) from learning new stuff certainly implies the kind of fearlessness that “Team Dauntless” might imply. Still, let’s ask one more question.

Question 3

> What prompted you to take on this project?

Well… our candidate was hired into a security team that hadn’t had an intern before. They were unprepared. It became quickly clear that there weren’t any clear tasks for her to take on. So, in the absence of guidance she started talking to the members of the team about problems they were facing to get a better lay of the land in search of problems she thought she might be able to take on. As this particular problem emerged, she started brainstorming with members of the team how it might be solved.

PowerShell arose early as a potential vector for a solution, so she taught herself over the course of a couple weeks. As more nuanced needs arose, she continued to seek guidance from more senior members of the team and, coupled with her own independent research, eventually arrived at the solution she finally rolled out.

The textbook definition of dauntless is “fearlessness and determination.” I can’t think of a story that better exemplifies these behaviors in a candidate and I’m really looking forward to this particular candidate joining our team.

When you’re interviewing the next member of your security team - consider this question. **Do they display the qualities of fearlessness and determination that will drive them to achieve great things in your organization?** Look for this, and you won’t be disappointed with the outcome.

--

This is the fourth part of a five part series on key areas of focus to improve security team retention. Read from the beginning, 5 ways to keep your security nerds happy.

About Expel
Expel provides transparent managed security. It's the antidote for companies trapped in failed relationships with their managed security service provider (MSSP) and those looking to avoid the frustration of working with one in the first place. To learn more, check us out at www.expel.io.