How to Build a Career in Cybersecurity
12.8.20

Thank you to our panelists!

Reginne Bonneau, CEO/Founder, RP Advisory - rbonneau@rbadvisoryllc.com
Joe Partlow, CTO, ReliaQuest - Twitter: @partlowjoe
Scott Noonan, SVP of Engagement, ReliaQuest - snoonan@reliaquest.com

What Experience Should You Have to Qualify for a Career in Cybersecurity?

- Each company is a little different - some have pre-requisites and some are more fluid
- Most important is demonstrating a **mastery** of the information, **passion and curiosity**
- For many companies, including ReliaQuest, a degree or certificate is helpful but not necessary if you have mastery of the material
- **Practicing and sharpening your skills on your own time demonstrates a commitment to the industry and desire to continually learn**
    - CTFs (Capture the Flag contests; an environment designed to test your hacking knowledge and skills) - helps to determine the perspective of cyber you prefer - defensive v. offensive. Typically the scores don't matter; the goal is to learn.
        - Defcon CTF - high profile one that earns you bragging rights!
        - Ctftime.org - good source for active CTFs to play
    - Practice in your homelab
- Certification and degree programs aren't always necessary but are beneficial:

    - They open opportunities for internships through higher ed and corporate partnerships like with AWS, Microsoft, others
    - Become important if you aspire to a corporate leadership role
    - Certification Resources Include:
        - Cybrary.it - free library to learn about certifications in cybersecurity
        - Cyberseek.org - for information on career paths
        - EC Council
        - International Association of Privacy Professionals
        - Cyber Florida
- Certifications with some hands on tech specific ones demonstrate experience -
    - Cloud security is a major industry gap with growing opportunity
    - AWS
    - Splunk
- Not all jobs are technical but provide a way to work in a dynamic field:
    - Business development
    - Marketing
    - Communications
- Your previous career experience could provide valuable experience and unique perspective that might benefit a career transition into cybersecurity
- A security clearance is helpful but not necessary. If you are in a current position with a clearance try to find a new opportunity before the clearance expires or shortly thereafter.
- LinkedIn is the number one recruiting resource - make sure your profile is up to date, reflecting professional work, side projects and interests.
- Keep your social media profiles clean. Remember: a cyber company can and will find things you may not want them to see. People have been passed up for opportunities because something on their social media profile does not reflect the values/culture of the company.

What to Avoid

What additional qualities would a great candidate demonstrate?

- Humility
    - Humility will serve you well
    - Cybersecurity issues are problems waiting to be solved, but require a willingness to learn, openness to new ideas and a collaborative mindset
    - Don't play up your skills to someone you don't know well; someone always knows more than you, and you don't know who you're talking to, especially at a professional gathering. The cybersecurity community is very small and well connected.
- Demonstrate that you're coachable - no one likes a "know-it-all" and no one can "know-it-all" in cybersecurity.
- Avoid using acronyms in general; often they have different meanings depending on the scenario or reference point.
- Culture fit is essential
    - Cyber can be a fast paced and stressful industry that requires fast and clear communication, collaboration and a great attitude.
    - Demonstrate this in every communication with *every* person at a company

Stay up to date on industry trends and news and networking opportunities

- Twitter - great way to follow "ethical" and "less ethical" hackers who will talk about what they've broken
- Follow virtual conferences and resources that are sharing the latest R&D
- Universities have student and alumni groups
- Search for cyber networking groups in your community to begin networking
    - BSides
    - Local Defcon groups
- Ask people in the industry - people are often willing to share their experience, knowledge and introduce you to others who could help you in your career path. Connect with them on LinkedIn.

What To Expect in the Typical Interview Process

- Technical vetting for transferable skills indicating you can adapt to and learn a new/proprietary technology
- Cultural assessment - will you fit the team chemistry
- Communication skills - assessing if you'll communicate clearly, effectively and in a timely manner (especially important in this industry where time is of the essence).
- Remember that all of your communications with any member of the team ultimately are seen/evaluated by the hiring manager. Always be prompt and professional with your communications.
- Background checks, drug screenings, sometimes personality tests are now the norm.

Preparing for the Future of Cybersecurity

- Companies are often hiring more for cultural fit and mindset rather than specific resume experience; you can learn any system with the right attitude.
- Data analysis via machine learning and automation will continue to become more essential to accelerating the pace of progress and to meet new challenges.
- Data privacy, compliance, Cloud computing, AWS is important.

Visit www.synapsefl.com to watch previous Libate & Learn episodes, connect with Florida's innovation community and learn more about upcoming Synapse events!

synapse
INNOVATION LIVES HERE