Epoch Sec

GETTING INTO CYBER SECURITY

TABLE OF CONTENTS

OVERVIEW

I wanted to write a guide (or basic mentoring document) to provide some initial areas to consider when thinking about entering the Cyber Security Field.

This document is not designed to train you. The purpose is give you direction on where to start. If you have any questions, or would like mentoring specifically for you, just reach out to me.

I will likely be routinely updating this document. So check back often!

BASIC NOTES

Below is a list of general thoughts about the Cyber Security Profession:

- Our field is very under filled. This means there are always plenty of job openings and positions available. Over the years, many new areas of Cyber Security have developed. Technology has developed as well, to a high degree. Therefor, more people are needed.
- This field, from my perspective also pays very well. Starting salaries are typically comfortable.
- There is not a day that goes by where I do not learn something new. So if you like learning, growing, new challenges, then this may be the profession for you.

STUDY AND LEARN

The thing about Cyber Security, is that there is a ton to learn. But that comes as you progress through your career. You do not need to know everything in the beginning. Here are some starting points for knowledge to learn. Again, you do not need to know all of these. When I began my career, I did not know much at all. I just slowly and steadily learned more over time.

- Start off by learning general knowledge about IT. For example:
    - Subnetting and IP addresses
    - TCP/IP Model
    - Types of Attacks (phishing, social engineering, ransomware, botnet, and many more)
    - What types of devices, appliances, communication happens in a typical network:
        - What is an email relay, or web proxy, or firewall versus an IPS, VLAN
        - What are virtual environments and cloud based solutions (AWS, Azure, etc)
        - Protocols and ports
        - Logging solutions
        - What is a SOC (Security Operations Center)
        - What is data protection
        - What types of storage solutions do environments use

        - What are some regulations and compliance requirements (HIPAA, PHI, ISO controls)
- A good tip is to look up Security Vendors
    - Look at what Security Vendors are selling, or building, or doing.
    - This will help you get more ideas about what to learn. You can even learn about specific tools or solutions they have.
    - It also helps give you insight into current trends, which may help you narrow your focus.

TRAINING RESOURCES

Here I will share some resources to take advantage of.

- Training Resources
    - Udemy:

        Watch Udemy for deals. They are kind of like Hobby Lobby. Courses can be expensive, but they are always running discounts and deals. You should never need to pay full price for a course.

        - First and foremost, here is a link for free options:
            - https://www.udemy.com/topic/cyber-security/free/
        - https://www.udemy.com/course/the-complete-cyber-security-course-end-point-protection/
        - https://www.udemy.com/course/network-security-course/
        - https://www.udemy.com/course/the-absolute-beginners-guide-to-information-cyber-security/
        - https://www.udemy.com/course/securityplus/
        - https://www.udemy.com/course/comptia-network-n10-008/
    - LinkedIn Learning

        I do not know the prices for LinkedIn Learning. But check it out for yourself. Also, your company may have an account already. If so, you would be able to log in with your work email.

        - https://www.linkedin.com/learning/paths/become-a-cybersecurity-professional?u=131945601
        - https://www.linkedin.com/learning/cybersecurity-awareness-cybersecurity-terminology?u=131945601
        - https://www.linkedin.com/learning/paths/starting-your-career-in-tech-cybersecurity?u=131945601
        - https://www.linkedin.com/learning/paths/prepare-for-the-comptia-security-plus-sy0-601-certification-exam?u=131945601
    - YouTube
        - I use YouTube on a daily basis. I am always watching videos whenever I can to learn something new or refresh my knowledge.
        - There are plenty of tutorials on there for a huge range of topics. Threat Hunting, using Kali Linux, various things about any OS, subnetting. If you can name it, there is a YouTube video. I personally like using the YouTube subscription so that a video

can play when I lock my phone, I have no ads, and I can download videos and watch them on a plane.

- One suggestion (and no I do not endorse anyone), would be to check out NetworkChuck. He covers and variety of topics and is fun to learn from and listen to.

CERTIFICATIONS

There are beginner certs and more advanced certs. I've listed out some of the key certifications below:

- CompTIA Security+
  - This is the most popular and needed certificate for entry level Cyber Security
- CompTIA Network+
  - A good complement to add to the Security+
- CompTIA A+
  - Covers a wide range of topics. Not as necessary as above certs, but useful to know the information. Recommend at least study material on the A+ cert.
- ITILv4
  - This is a certificate for the overall understanding and knowledge of IT management in general. It covers many topics to help and IT environment be managed and designed well. It is not an entry level certificate, but I did get it rather early in my career.
- CISSP
  - This is the Certified Information Systems Security Professional. This is the main certificate achieved by advanced Cyber Security Professionals. You have to pass the exam, have a minimum of 5 years of officially working in the field, and have someone who is already certified to sponsor you.

- CCNA
  - Cisco Certified Network Associate Certification. This is a great certification that gets more detailed on Networking and could be a useful cert for individuals interested in this direction.
- C|EH
  - Certified Ethical Hacker Certification. This is a great certification individuals interested in ethical hacking, forensics, and similar careers.

JOB ROLES

I thought I would list out some common positions and roles for you to see the possibilities for the directions you can take.

- Security Technician/Administrator/Specialist

    - I typically suggest looking for these roles for your first entry level job. You are typically managing security solutions already implemented, or with the help of vendors or more tenured architects/engineers. Your general day to day work would be maintenance, monitoring, or implementing changes based on requests from other teams.
- Now here is a list of possible areas you can move into as you progress. That is not to say, if something sticks out to you, that you couldn't start out in one of these roles.
    - Networking (the other side of IT, versus Host/Endpoint)
    - Host/Endpoint (This would be working more with workstations and servers that employees are using)
    - Software Development or Engineering
    - Architecture
    - Risk Analysis
    - Auditing or Compliance
    - Intelligence
    - Threat Hunting
    - Forensics / Incident Response
    - Consulting
    - Cyber Crime Investigator
    - Choosing between Govt or Commercial Sectors
    - Management
        - CISO – Chief Information Security Officer
        - CIO – Chief Information Office (Typically leading the CISO and all other roles in an IT team)

CONCLUSION

If you want help or mentoring, please reach out to me. I am more than happy to help. I can give you guidance. I can help you understand something. I can help teach you a topic. Whatever you need, let me know.