Roadmap to cyber security career for beginners

Cyber-security is the study related to the security of network devices and systems and their sensitive data from the attackers. Here we are going to discuss the path or road to reach a cyber-security professional path for beginners. Now, most of you are standing at a point of completing graduation or working in some jobs, but deeply like to become a cyber security engineer.

A cyber security profession is a highly paid job and has a huge number of diversities to divert inside the cyber-security. The job data says the need for

cyber security engineers are increasing rapidly and many organizations are offering huge payment for cyber security experts.

Don't select the cyber security profession if you are not much interested in networks and devices and the packets and all. Also, a security engineer profession has to face different challenges every day that too in critical situations, so select the cyber security career if you are really interested in it. Let us begin the journey, of how to become a cyber security professional.
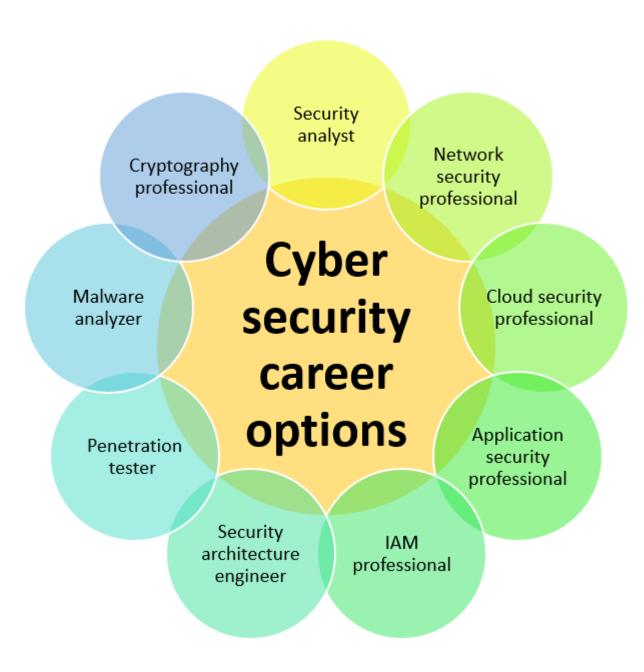
What is cyber security?

It is a basic question as it provides the security for the network devices and systems that are working in cyberspace from the attacks which are done by cybercriminals. The definition is simple and lets us see how it becomes while going in-depth.

According to data and graphs, the cyber attacks are increasing every day as almost all type of users and organizations are entering to cyberspace for their daily routine and the need for cyber security experts are at peak as around 3.5 million jobs are available around the globe and it is the perfect time to start your career in it.

Cyber security career options

We already discussed that cyber security is a vast area with a lot of diversification inside it and let us see many job types are coming under cyber security. According to the employment data around 400000 professional

shortages is there in the US only for a cyber security job. Let us see the job types in cyber security

1. Security analyst

2. Network security professional

3. Cloud security professional

4. Application security professional

5. Identity and Access Management (IAM) professional

6. Security architecture engineer

7. Penetration tester

8. Malware/forensics analyzer

9. Incident response analyst

10. Cryptography professional

11. Security train professional

12. Security auditor

13. Governance, Risk and Compliance engineer

Please understand these are not the full list as it is beyond our scope. These are some of them in the list and there are a lot of more career options in cyber security

Getting started in a cyber security career

```
Qualification  →  Skills  →  Learn basics
                                  ↓
Select your    ←  Prepare   ←  Read as many
path              yourself      as you can
  ↓
Look for       →  Attend      →  Practice
certifications    conferences
                  and meetings
```

1. Qualification

To start with you need a basic qualification as graduation in information technology or computer science-related course or any equivalent graduation as a basic building block. Please keep in mind there is no need to be engineering graduation it can be any graduation that is related to Computer science.

2. Skills

Next, you need to check the skills that a cyber security professional has which is really important to handle the security threats that are really

happening suddenly and should be resolved in real-time as soon as possible.

The skills needed for a cyber security professional are

1. Have knowledge in programming languages like java, python, c, and know the operating system Linux.

2. Have the ability to work under pressure

3. Problem-solving skill

4. Good communication skill

5. Basics of network and internet

3. Learn basics

Once you reach this milestone then your track to becoming a cyber security professional is half done. Now you have to learn the cyber security basics, OSI model of networking, terminologies of the network, Working of the internet, Hacking tools, Security policies, Type of threats, etc for getting the next building block of your path. We prefer to refer to any online free course to get this knowledge. If you are interested you can refer to our tutorials as it is refined and simple to learn about these all.

4. Read as many as you can

In this stage, you have to increase your knowledge as much as you can. Read a maximum number of online courses and tutorials available. If you are

ok you can take paid courses at this stage and update your knowledge about the latest security measures hacking methods viruses and threats the world is facing. You can check tech magazines for such knowledge.

5. Prepare yourself

This is an important milestone as you are going to start practicing. Make your lab in your computer and don't forget to use only Linux for preparing the lab. Go and check simple hacking and security tools at first. Keep in mind to get maximum knowledge before practicing a tool. Also, be careful about the threats while checking for the tools. Work with firewalls and security measures to get more knowledge.

6. Select your path

In this milestone, there will be a lot of roads you can see. As we discussed above there are a lot of cyber security jobs and career options. Never take an option to look only at rewards, select one which you are interested in and confident to go further. Once you select the path, refine your search and practice according to that path.

7. Look for certifications

Now you are like a pro in your knowledge and practice but that is not enough for an organization to select you. You have to take any certification depending on the path you selected for impressing the organization. Never jump to this step without reaching the previous milestones as it will make your journey fail.

CompTIA Certifications

- A+

- Network+

- Security+

- Linux+

- CASP + : CompTIA Advanced Security Practitioner

- CySa+ : CompTIA Cybersecurity Analyst

EC Council Certifications

- CEH: Certified Ethical Hacker

- CHFI: Computer Hacking Forensics Investigator

- ECSA: EC-Council Certified Security Analyst

- LPT: Licensed Penetration Tester

ISACA Certifications

- CISM: Certified Information Systems Manager

- CISA: Certified Information Systems Auditor Cisco Certifications

- CCNA Routing & Switching: Cisco Certified Network Associate

- CCNA Security: Cisco Certified Network Associate

ISC2 Certifications

- CISSP: Certified Information Systems Security Professional

- SSCP: Systems Security Certified Practitioner

- CCSP: Certified Cloud Security Professional

- CAP: Certified Authorization Professional

8. Attend conferences and meetings

Try to get more and more knowledge about the network trends and their threats by attending important conferences and meetings that will help you to become smarter and smarter and be professional. Attending the meetings and conferences is worth not only for building knowledge but also for getting more and more relations which will be good in your career.

9. Practice Practice practice!!!

This is a never-ending milestone in your career as you have to gain knowledge and practice more and more all-time to become more worthy in the industry, do more certifications, and make more and more achievements in the career

How much Cyber Security has reached now?

Now you understand the story behind the trigger the formation of cyber security. That Creeper and Reaper programs were made just for fun as it

doesn't cause any problems to anyone. But as computers and networks made an immense development, criminals start to think to use the loopholes for stealing user data and even destroying a network or a computer. When the internet and cyberspace become more and more popular then came the hackers who hack many systems and user data which is very dangerous. A German citizen hacked even many military computers and was able to access its data, even from the pentagon systems.

In 1987: the antivirus started to be used for commercial activities and available to the common man who was able to buy an antivirus for his computer.

1. Andreas Luning and Kai Figge were behind the first antivirus which is called UVK mean Ultimate Virus Killer. After that NOD antivirus was created

2. John McAfee from the United States found the McAfee

3. In the same year, the Bernd fix caught a wild virus which is named as Vienna virus. Which is supposed to be the first malware.

You heard about Morris worm or Internet worm. It was a man named Robert Morris who invented a computer worm with a crooked intention to know how

many computers there are on the internet. He wrote a program to know that. Morris worms can infect a system multiple times and start running in the system making it slow and destroying the system eventually. There are millions of stories like Morris and different hackers who made different computer viruses and malware. IN the present situation even some countries are making malware and worms which are able to get the information from other countries' systems. In the **1990s**: there were drastic changes in the internet and cyberspace which make the world go online and some important issues also come with online changes.

1. First Polymorphic Viruses detected: Polymorphic viruses are next-gen viruses that change a file and spread but keep the original program intact so no antivirus till that date can find it.

2. Another virus named Disk Killer was detected by a British magazine which infects and destroys millions of computers.

3. It made the establishment of EICAR that is the European Institute for Computer Antivirus Research.

Now we have a different range of anti-viruses and anti-malware to protect from the known viruses and worms. But we can hear the news of new viruses and worms which make us understand the need for cyber security.

GOOD LUCK!!!