WHOAMI

$: echo whoami

whoami

$:whoami |figlet

```
 ____ _    ___     __ __
|  __/ \  |  _ \    \ \/ /
| |_/ _ \ | | | |___\  /
|  _/ ___ \| |_| |____/  \
|_|/_/   \_\____/    /_/\_\
```

Cybersecurity, or information technology security (IT security) is the protection of computer systems and networks from information disclosure, theft of or damage to their hardware, software, or electronic data, as well as from the disruption or misdirection of the services they provide.

Careers in Cyber Security

Cybersecurity experts work in every size company and industry to protect organizations from data breaches and attacks

1. Security Software Developer

Security Software Developers build security software and integrate security into applications software during the design

and development process. Depending on the specific position and company, a security software developer might oversee a team of developers in the creation of secure software tools, develop a company-wide software security strategy.
PayScale reports security software developers earn an average annual salary of $72,965

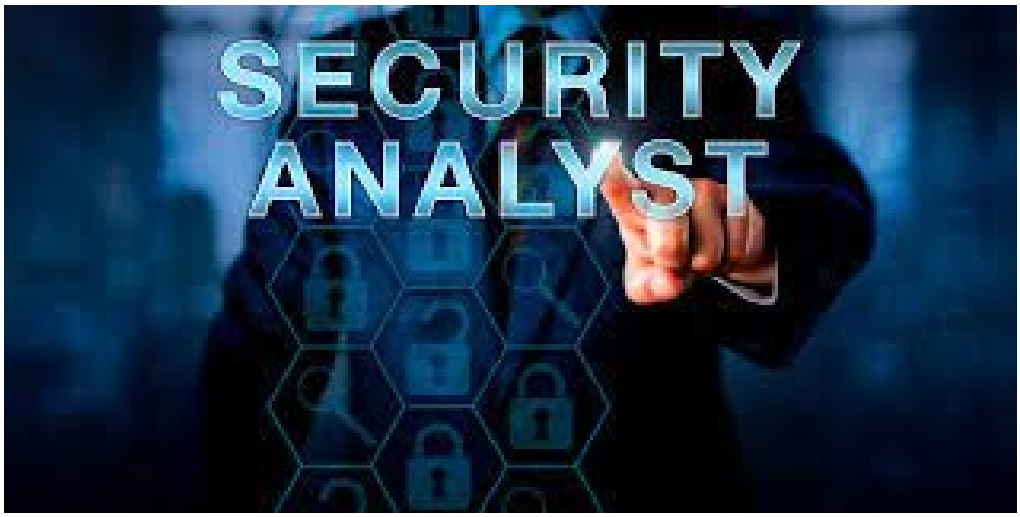
2. Security Architect Career Path

If you're enthusiastic about problem-solving and formulating big-picture strategies, the security architect career path is for you. A security architect is meant to create, build and execute network and computer security for an organization. Security architects are responsible for developing complex security framework and ensuring that they function effectively. They design security systems to counter malware, hacking and DDoS attacks.
For a Security Architect Average annual salary is $153,439 with an average monthly pay of $12,786.

3. Security Consultant

A security consultant is a catch-all cybersecurity expert. They evaluate cybersecurity threats, risks, problems, and give possible solutions for different organizations and guide them in protecting and securing their physical capital and data. Security consultants must not be too rigid and must be tech-savvy
The average salary for a security consultant is $81,261 per year in the United States.

4. Information Security Analyst

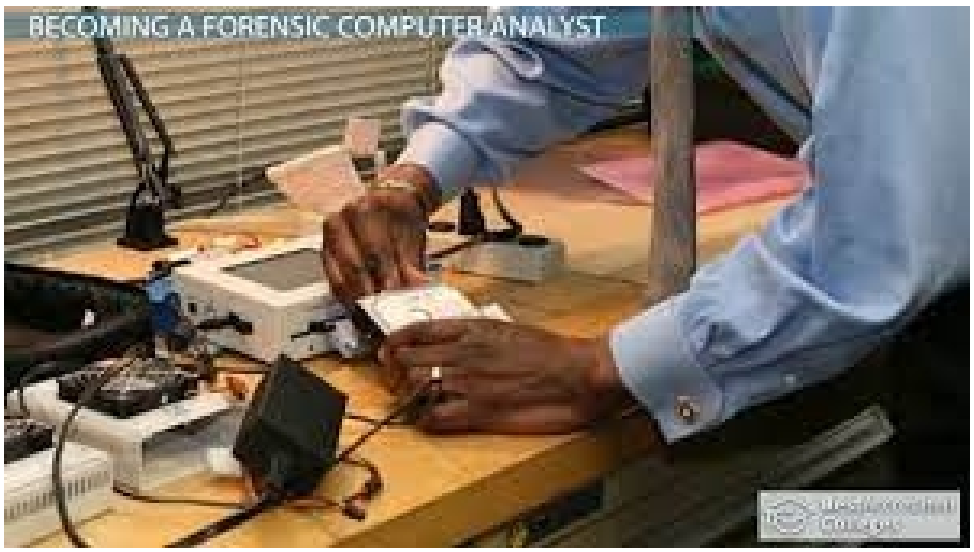


Information Security Analysts are the front-line defense of networks.nformation security analysts plan and carry out security measures to protect an organization's computer networks and systems. Information Security Analysts put firewalls and encryption in order to protect breaches, constantly monitor and audit systems for unusual activities.
The average salary for a Cyber Security Analyst is ₦1,199,508 in Nigeria.

4. Ethical Hackers

Ethical hackers normally hold a CEH certificate and are given license by their employers to try and infiltrate the security of their system. The idea is that they use the same techniques as malicious black hat hackers to test existing security protocols; if they are successful, upgrades can then be developed and implemented.
The average salary of an Ethical Hacker in Nigeria is ₦3,000,000 per year.

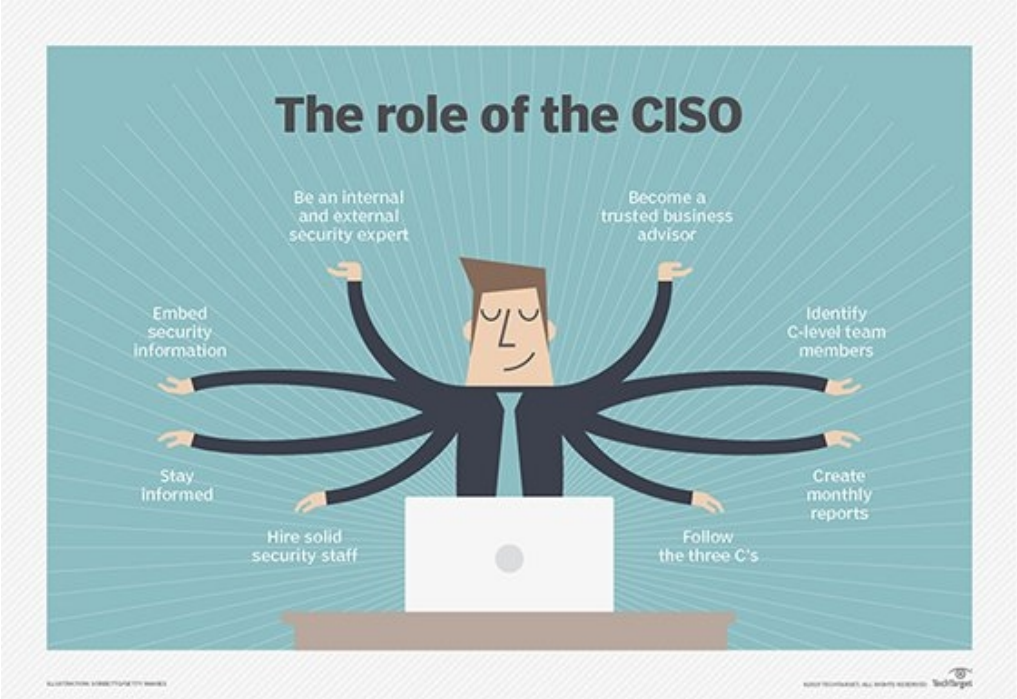
6. Computer Forensics Analysts



Forensics analysts focus on cyber-crime, an ever-growing phenomenon. They work with law enforcement agencies in both public and private sector organizations and are asked to

undertake a wide variety of tasks, including:Recovering deleted files, Interpreting data linked to crime, Analyzing mobile phone records, Pursuing data trails.
Computer forensic analysts must keep a well detailed records of their investigations, and often provide evidence in court.
The average salary for a computer forensic analyst is $61,667 per year in the United States.

7. Chief Information Security Officer



The Chief Information Security Officer is normally a mid-executive level position whose job is to manage the affairs operations of a company's or organization's IT security division. CISOs are usually responsible for planning, coordinating and directing all computer, network and data security needs of their employers. CISOs work directly with the management to determine an organization's custom cybersecurity demands. The CISOs are usually saddled with the responsibility of assembling an effective staff of security professionals, which means that the position requires an individual with a strong background in IT

security architecture and strategy, as well as effective communication and human resource skills.

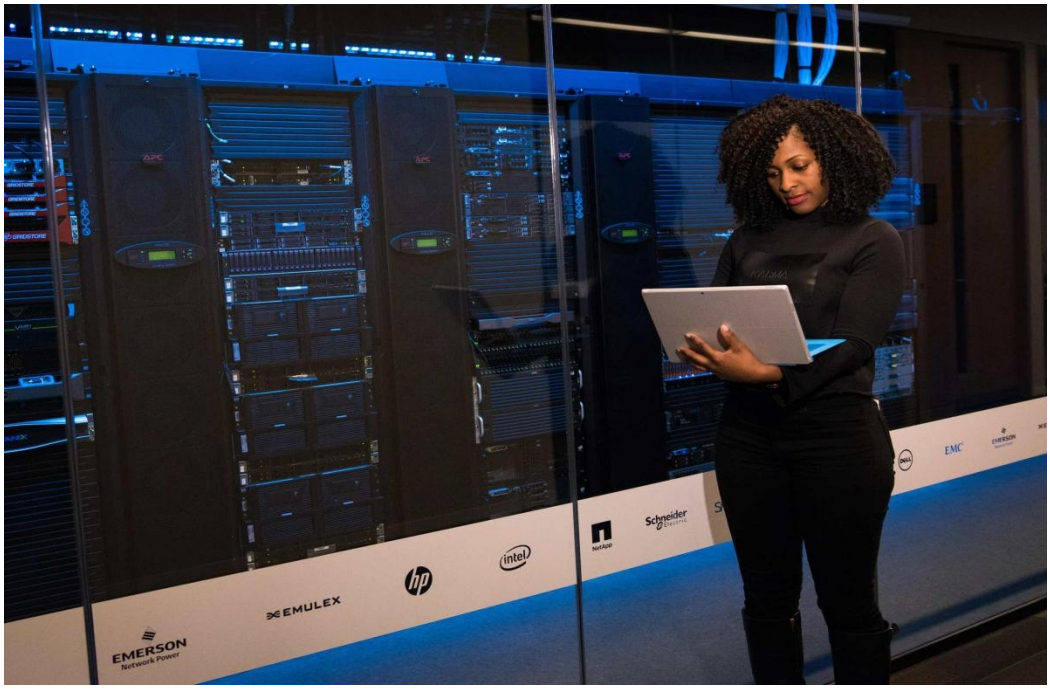
The base salary for Chief Information Security Officer ranges from $199,972 to $264,487 with the average base salary of $229,010.

8. Penetration Tester

Penetration testing is the proactive authorized employment of testing procedures on the IT system to identify system flaws. A penetration tester usually attempts to (with permission) hack into a computer and network systems to pre-emptively discover operating system vulnerabilities, service and application problems, improper configurations and more, before an intruder cause real damage. Penetration testers must be highly skilled, often using testing tools of their own design, to “break into” the systems under watch. Penetration testers are required to keep accurate records of their activities and discovered vulnerabilities.

The average salary for a penetration tester is $114,989 per year in the United States.

9. IT Security Consultant



IT security consultants meet with clients to advise them on how to protect their organizations' cybersecurity objectives best efficiently and cost-effectively. IT Security Consultants are often employed by smaller firms and agencies that cannot afford to handle their security issues in-house but are also employed by big corporation to supplement their security teams and provide an impartial outside perspective to current systems challenges. The average pay for an IT Security Consultant annually is $115,767 and monthly $9,647.

10. Security Systems Administrator

A security systems administrator's responsibility is a bit similar to many cybersecurity jobs i.e., installing, administering,

maintaining and troubleshooting computer, network and data security systems. The main distinction between security systems administrators and other cybersecurity professionals is that the security systems administrator is normally the person in charge of the daily operation of those security systems. The regular tasks include systems monitoring and running regular backups, and setting up, deleting and maintaining individual user accounts. Security systems administrators are usually often involved in developing organizational security procedures. As you can see, there are endless paths your cybersecurity career can lead you down.

BUILDING A CAREER IN CYBER SECURITY

1. **Work out if it's right for you:** You can enter the field from school, college, from another tech discipline or, with enough planning, persistence and personal development, from an unrelated discipline. But before you start the journey, you need to make sure it's a good fit. You'll need passion to make a success of it, so don't just follow the paycheck.

2. Narrow down your options: The days of the "security expert," who knows about everything, are over. The focus is now on niche specialists. These days, you can specialize in areas such as web application security, forensics, compliance/risk management, auditing, network security and identity management. You'll find a good list of roles here.

Choosing a specialty won't stop you from moving to another later in your career.

3. Self-development can get you a long way fast: To defend something from attack, you need a good grasp of how it works. So before you wade too deeply into security matters, make sure you know the technology.

Get practical experience applying what you learn

Information security is a good example of a career **where experience counts for more than formal education**. Hackathons, capture-the-flag exercises or hacker playgrounds are a good way to try out your skills for real. Once you're a step further on, you can find software bugs for vendors and earn in the process.

4. Getting certified deepens your knowledge and opens more doors: For some people, self-development is enough to get their career going, but others will want to add formal training and certifications.

If you've got a degree in a computer science or cyber security from a credible institution, that's a big help, but otherwise or in addition to that there's a range of organizations offering certifications recognized industry-wide.CompTIA, (ISC)², ISACA, EC-Council, GIAC, Cisco, Microsoft, Security+, Certified Ethical Hacker, offered by EC Council.

5. Work hard at getting that first job: Chances are your first information security job won't come quickly or easily.

With any luck, your social media networking will get you a foot on the ladder. Otherwise, you'll be in the same cycle as every other job hunter: search, apply, repeat.

Create a resume that will get attention

Your resume is most likely to be the first thing a potential employer sees, so take time to get it right.

Experience needs to be front and center. The areas we described above are all relevant, so describe them in detail.

6. Don't stop when you've just started: Building a successful career in information security is a long-term commitment. Self-learning doesn't stop and, since you'll face more responsibility and greater challenges, it takes on even more importance. Rather than use social media or conferences to soak up knowledge, you can gradually move towards becoming a contributor.

With the careers listed above and tips in building them, I would like each and every one of you to run the command 'whoami'(who do you want to become?) on your inner terminal (yourself) then pipe the result out to figlet(in a stylish way) for the world to see.

Start NOW!!!

Remember *"to feature in a future you have pictured you have to structure it....."*

AJEIGBE FADILULAH OLAYINKA