CYBER SECURITY

alert(`Hello ${user.name}`);

From ordering a taxi to booking a room. There are billions of bytes of information moving every second

The Internet has gotten big. Scary BIG. The average user is not aware of all the dangers lurking on the Web

WHY BOTHER?

With the giant ocean of information and data around, a golden age has been created for black hat hackers. There are more than enough vulnerabilities to exploit. Basic CySec knowledge is a must in this day and age

WHAT'S IT?

The name says it all. It's the practice of keeping a company or your data safe from malicious attackers with harmful intentions. Be it hardware or software

As companies get bigger and bigger and generate more and more data, cyber security has become mandatory. Hell yeah job security! Or is it security job.....

CIA TRIAD

CONFIDENTIALITY

Ensuring privacy to prevent the wrong people from accessing your information. Only grant access to authorized persons

INTEGRITY

If proper systems are in place, attackers will have a hard time getting in. Small bit of security goes a long way

AVAILABILITY

Is access to your data restricted to only authorised people?

PREVENTION

Safety is only a feeling. If someone wants to get in, they will get in. It's our responsibility to implement systems, practices and incident response plans.

These systems hinder any attacker. The longer they take, the more time you will have to launch a counter attack!

WE PROTECT FROM

The CIA is used as a core reference (The Three Pillars Of Security) for protecting against unauthorized access, deletion and modification. All companies following proper CySec regulations follow The Three Pillars.
How long can a building stand without pillars for support

I'M IN

Once a hacker is in, there's really not much you can do. Pulling the cables always works on the other hand .... (seriously, don't ever do that....)

Doing Risk Assessment is the staring point for understanding where the vulnerabilities are that a potential hacker could exploit.

ASSESSMENTS

Threat +

Anything that could damage or expose the data of a company is cosidered a threat. This could be from natural, intentional or unintentional threats

Vulnerability =

Any weakness in a data asset that can be exploited by an attacker is considered vulnerable. This could be bugs/defects in software or hardware

Risk

Risk Management is key to cybersecurity. Risk refers to the potential loss or damage when a threat exploits a vulnerability. We limit the collateral

ROADMAP

necesSkills.map(skill => (skill.learn()));

100 hours of pure focus into a practice would put you in a decent skill range

3 months, 2 hours a day

CODE SECURITY

Creating scripts that track a user's activity would make it easier to determine suspicious activity when an attacker strikes. Alerts could be sent to admin when there is large file download or unusual login methods. Immediate credential changes could be executed

Finance tracking app example

LINUX

Most secure OS out there. A must. Kali Linux is your best friend. Used for Pen Testing and System Analysis
Red Hat Distro is also a big one

PYTHON

It's the biggest scripting language out there. Gotta learn that lingo
Nessus is the threat assessment tool you'll most likely be using

CERTS

Paper gets you far, skills get you further

CEH (Certified Ethical Hacker)
OSCP (Offensive Security Certified Professional)
CISA (Certified Information Security Auditor)
GCIH (GIAC Certified Incident Handler)
Certified Information Systems Security Professional (CISSP)

You can work at the NSA bruh...

SOFT SKILLS

You will be working with a lot of people that are not technically trained.

You will need communication skills to properly convey complex technical jargon into understandable concepts

IMPLEMENT

Learning how to assess a business and finding the potential security risks is a big part of what you will do,

When you start with security, you begin with writing scripts that automate certain security tasks. Backups, Authentication

HABITS

Eagerness to dig into technical questions and examine them from all sides.
Enthusiasm and a high degree of adaptability.
Strong analytical and diagnostic skills.
A current understanding of common web vulnerabilities.
Maintaining awareness and knowledge of contemporary standards, practices, procedures and methods.

MONEY

This is a baller profession. You can make F U Money in 5 years of consistency

And if you have a head on your shoulder with some grey matter, you could write all your work tasks into batch scripts...

Salary range of R35 000 and jumps up to R95 000-R125 000