

Understanding Cybersecurity (2019)

by

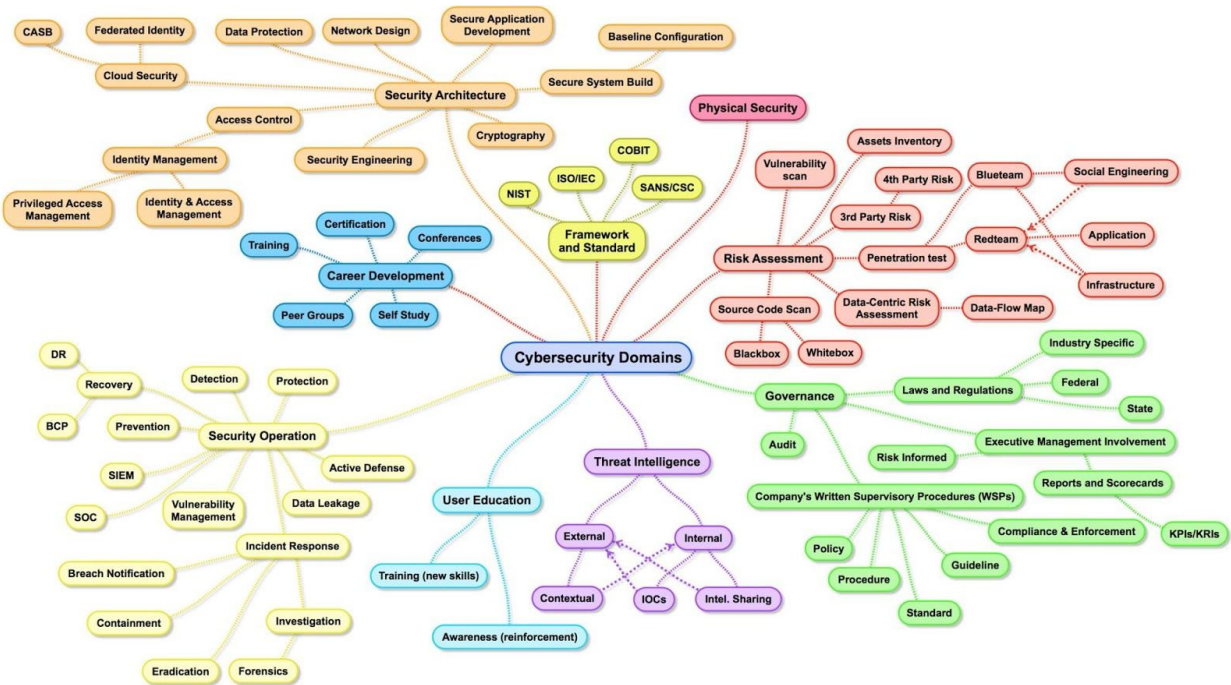
X1KHgM@keemail.me

Cysec Overview
Resource Guide
Summer 2019

Table of Contents

Page 3	-----	Cybersecurity Job market overview
Page 4	-----	Enterprise scale application hardening
Page 5	-----	Learning Python
Page 6	-----	Industry Certifications
Page 7	-----	Networking Job Market overview
Page 8	-----	Bug bounties

Cybersecurity Job market overview



Positions in Cybersecurity:

Security Architect
 Security Analyst
 Cybersecurity Analyst
 Threat Analyst
 Security Engineer
 Penetration Tester
 Incident Response Analyst

IT related search terms:

SOC Analyst
 Systems Administrator
 Information Assurance Specialist
 Network Administrator
 Help Desk Technician
 IT Help Desk Technician

Enterprise scale application hardening

Everything in [Git](#) is checksummed before it is stored and is then referred to by that checksum. This means it's impossible to change the contents of any file or directory without [Git](#) knowing about it.

[Gitlab](#) provides enterprise scale source code management

Git is Linux so learning [the basics of Linux](#) terminal commands is how you can learn Git.

The Terminal

Navigation e.g. "cd ~"

File Manipulation e.g. "mv [source] [destination]"

Linux supports unix-style filesystem permissions, which restricts who can read and write certain files.

|

E.g. "chmod 700 apple.txt"-----Only you can read, write to, or execute apple.txt

Slack (Enterprise scale Group chat)

Big companies save time with Slack by securely collaborating across teams, departments, offices and countries.

Learning Python:

I recommend Datacamp; This is a paid subscription service. There is a free trail.

<https://www.datacamp.com/tracks/python-programming>
<https://www.datacamp.com/tracks/data-scientist-with-python>

To get straight into exercises:

<https://www.w3schools.com/python/exercise.asp>
https://www.w3schools.com/python/showpython.asp?filename=demo_variables1
https://www.w3schools.com/python/python_examples.asp

To DL Python:

- 1). <https://www.python.org/downloads/>
- 2). As soon as the file downloads open it and the Python installer window will open
Click "ADD Python 3.7 to PATH"
- 3). Click install now then continue by clicking "Next" until it finishes.

Python runs in the command line "cmd"

- 1). Press the Windows key or click the Windows icon on the bottom left of your computer
- 2). type "cmd"
if you want you can right click the program and "pin to taskbar"
- 3). press enter
- 4). Type "python" and version information will be displayed in the command prompt.
- 5.) Type "exit()" to end the python interpreter session.

Industry Certifications:

[CompTIA Security+](#) is the first security certification IT professionals should earn. It establishes the core knowledge required of any cybersecurity role and provides a springboard to intermediate-level cybersecurity jobs.

EXAM OBJECTIVES (DOMAINS) The table below lists the domains measured by this examination and the extent to which they are represented:

DOMAIN	PERCENTAGE OF EXAMINATION
1.0 Threats, Attacks and Vulnerabilities	21%
2.0 Technologies and Tools	22%
3.0 Architecture and Design	15%
4.0 Identity and Access Management	16%
5.0 Risk Management	14%
6.0 Cryptography and PKI	12%

Other certifications of interest

[CompTIA Network+](#)

EXAM OBJECTIVES (DOMAINS) The table below lists the domains measured by this examination and the extent to which they are represented:

DOMAIN	PERCENTAGE OF EXAMINATION
1.0 Networking Concepts	23%
2.0 Infrastructure	18%
3.0 Network Operations	17%
4.0 Network Security	20%
5.0 Network Troubleshooting and Tools	22%

Networking Job Market overview:

Junior Network Administrator

Network Engineer

Network Field Technician

Junior System Engineer

IS Consultant

Network Field Engineer

Computer Technician

Help Desk Technician

System Engineer

Network Support Specialist

Network Analyst

Bug bounties:

Receive compensation for finding or resolving security vulnerabilities

The pay for **one bounty** is between \$50 - \$20,000+

Compensation amount normally increases by increments of \$500

500

1000

1500

2000

...

Bounties have been offered by almost all large companies:

Tesla

Apple

The DoD

Amazon

Twitter

Facebook

AT&T

Verizon

Google

Microsoft

In April 2018, the organization previously known as Oath Inc. shelled out **\$400,000** to **40 participants**

After the success of these bug bounty events, the company created a consolidated bug bounty program, which paid out **\$5 million** in 2018

Google's Vulnerability Rewards Program dates back to 2010. It has since paid out more than **\$15 million**

The largest bounty awarded to a single person that we know of is **\$200,000** in 2012.

https://hackerone.com/hacktivity?sort_type=latest_disclosable_activity_at&filter=type%3Aall&page=1&range=forever

<https://www.guru99.com/bug-bounty-programs.html>