

Skill Up with IBM; How to Start Your Career in Cybersecurity

Version 1| October 21, 2021

Today's Topics

- Why Cybersecurity? Oscar Calderon
- What will I do all day? Kenneth Gonzalez
- Now What? Coreen Ryskamp

What is Cybersecurity?

- Focus to protect data from cyber attacks and data breaches (Confidentiality, Integrity, Availability)
- In 2020, the average cost of a data breach was **USD 3.86** million globally, and **USD 8.64** million in the United States
- Prevent bad reputation and enable operations (Protect to Enable)

Why Cybersecurity

- Everchanging Environment
- 0% Unemployment rate (3,5 Million Openings by 2021)
- Digital Transformation (COVID pushed this forward)
- Jobs with Real Impact

A day in a life

Cybersecurity Analyst / Pentester

1.7m

Average number of outstanding
vulnerabilities in client environments

Source: : X-Force Red vulnerability management client statistics

Pentester

What could they do...

Application

- Web
- Mobile
- Terminal
- Thick-client
- Mainframe
- Middleware
- Cloud

Network

- Internal
- External
- Wireless
- Other radio frequencies
- SCADA

Human

- Physical
- Social engineering
- Phishing

Hardware & embedded devices

- IoT
- Wearable tech
- Point-of-sale
- ATMs
- Self-checkout kiosks

Now the Cybersecurity Analyst point of view

Identify threats

Understand the risk and why the threat is relevant

Understand the context of the threat

Escalate and alert

Recommendations and continuum monitoring



Now What?

What do I need?

Don't be afraid! You need to believe in yourself to make it happen.

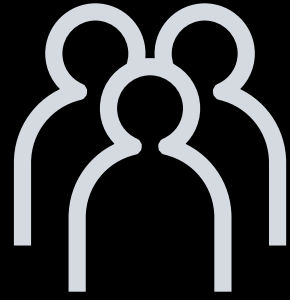
Motivation to learn. There's something new to learn every day.

Develop People Skills. You need more than technical knowledge to be a good Security Specialist.

Technical Skills. Cybersecurity requires knowledge in many technical fields. We must know a little about everything



People Skills



- Problem Solving, Critical Thinking.
- Communication Skills.
- Be able to work with minimum supervision.
- Time Management (SLAs, SLOs)
- Standards and methodologies:
 - Agile
 - Scrum
 - ITIL



Technical Skills



- Computer Networks.
- Linux Operating Systems.
- Windows Operating Systems.
- Programming and Software Development.
- Analysis of payloads and events.



Common Cybersecurity Roles

- Security Analyst
- Pentester
- Threat Intelligence Analyst
- Incident Responder
- Cyber Threat Analyst

Stay updated!

Besides having technical knowledge, you need to understand what's happening in the Cybersecurity world.

Look for trusted sources:

[National Institute of Standards and Technology \(NIST\)](#)

[IBM X-Force Exchange](#)

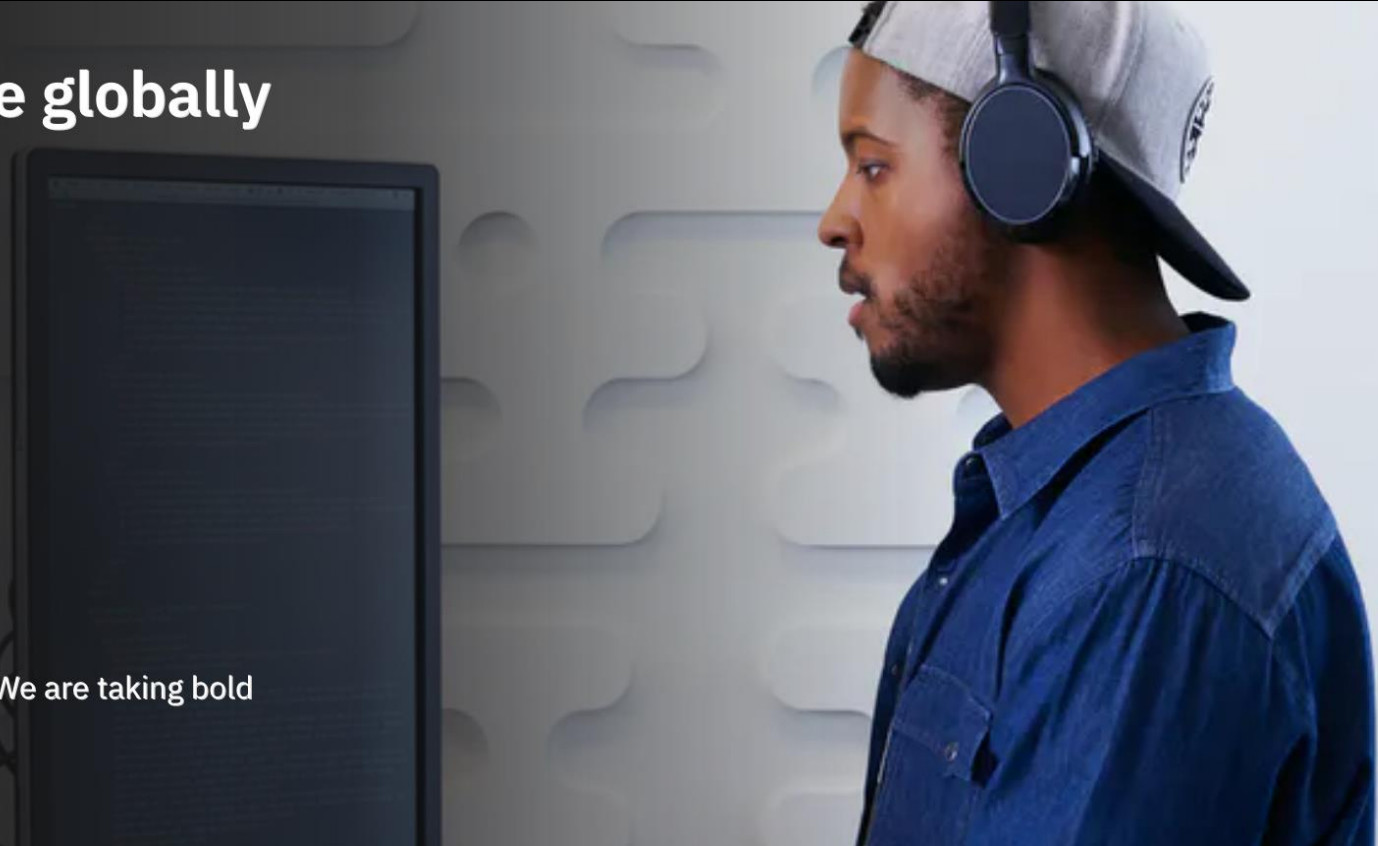
[Cybersecurity & Infrastructure Security Agency](#)



IBM's Skills Initiative

**We're skilling 30 million people globally
by 2030**

Closing the skills gap is the biggest opportunity of the decade. We are taking bold action to achieve this.



Resources

- [IBM Cybersecurity Analyst Professional Certificate on Coursera](#) (First month Free)
- [IBM Cybersecurity Fundamentals on edX](#)
- [IBM Skillsbuild](#)
- [IBM Security Learning Academy](#)
- [IBM Security Community Skills and Learning](#)

Thank you

Follow us on:

ibm.com/security

securityintelligence.com

ibm.com/security/community

xforce.ibmcloud.com

[@ibmsecurity](https://twitter.com/ibmsecurity)

youtube.com/ibmsecurity

© Copyright IBM Corporation 2021. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty, of any kind, express or implied. Any statement of direction represents IBM's current intent, is subject to change or withdrawal, and represent only goals and objectives. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.

