Cybersecurity Careers

Career Options, Paths and Preparations for Future Success

Welcome

When you think of countries hacking into others, what are the Top 5 countries in terms of hacking capabilities…the Usual Suspects?

Sources:

- https://www.zdnet.com/article/hacking-and-cyber-espionage-the-countries-that-are-going-to-emerge-as-major-threats-in-the-2020s/
- https://cybernews.com/editorial/the-worlds-most-dangerous-state-sponsored-hacker-groups/
- https://news.clearancejobs.com/2022/10/17/the-not-so-secret-cyber-war-5-nations-conducting-the-most-cyberattacks/

This presentation is derived from information I have gained throughout my career. The perspectives I am sharing are my own and are not necessarily that of my employer, Fulton Bank.

Cybersecurity Career Options

- Security Analyst (Blue Team)
- Penetration Tester (Red Team)
- Threat Intelligence Analyst
- Incident Responder
- Threat Hunter
- Security Awareness Educator
- OSINT Investigator
- Malware Reverse Engineer
- Mobile Device Forensicator
- Vulnerability Researcher
- Identity & Access Management Analyst
- Digital Forensic Analyst
- Many more!

Interests that may fit well:
- Gaming
- Lifehacking
- Legos & other gadgets
- Mysteries – movies and/or books
- Puzzles or Magic
- EMS
- Exploring
- Math
- Teaching
- Child care
- Art
- Music

Pathways to a Cybersecurity Career

- Educational requirements
  - Historical standard: 4-year IT, Computer Science, Cybersecurity degree
  - However: college degrees becoming more optional
  - Advantages of a 4-year degree

- Never stop learning!

- Examples of cybersecurity career journeys
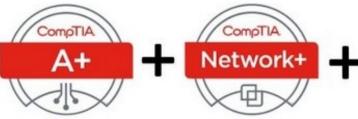
Cybersecurity Certifications

Building Your Technical Ninja Cred

Practical experiences

- DIY cybersecurity/home lab
- Volunteering
- Internships

Skills to develop

- Excel(!)
- Coding (scripting languages/automation)
- Packet Analysis
- Regular Expressions

Soft Skills that Foster Success

- **Communication** – translating cybersecurity into common language

- **Customer Service** – users happy to come to you, not try to go around you

- **Social Engineering** – understanding human vulnerabilities

- **Professional Networking** – being a lifeline to build your own lifelines

- **Reducing Cognitive Biases** – how to better recognize and learn what you don't know so you can make better decisions

Continuing Your Cybersecurity Exploration

- Traditional Continuing Education Sources:
  - ISC^2
  - ISACA
  - CompTIA
  - SANS
- Topical Focused:
  - TrustedSec
  - Applied Network Defense
  - Black Hills Infosec/Active Countermeasures/Anti-Syphon

Resources for Additional Career Exploration

- SANS – New to Cyber Field Manual
- National Cybersecurity Alliance Career Guidance
- Building a Home Lab – many Internet sources
  - SANS
  - Black Hills Information Security
  - PSU
- Slack and Discord channels