Cyber Certs: Navigating Your Letter'ed Path

TAYLOR KAUFMAN, CISSP, ADVANCED THREAT HUNTER

Mentimeter poll

Quick disclaimer

- Any viewpoints in this presentation are mine and mine alone and do not necessarily reflect the opinions or believes of any companies or colleagues I work with or have worked with in the past
- I am not endorsed by any company to promote certification material or courses
- Certifications mentioned are not the end all be all and there are many others not mentioned which may suit goals better
- **Your experience may differ—and that's a good thing!**

About me

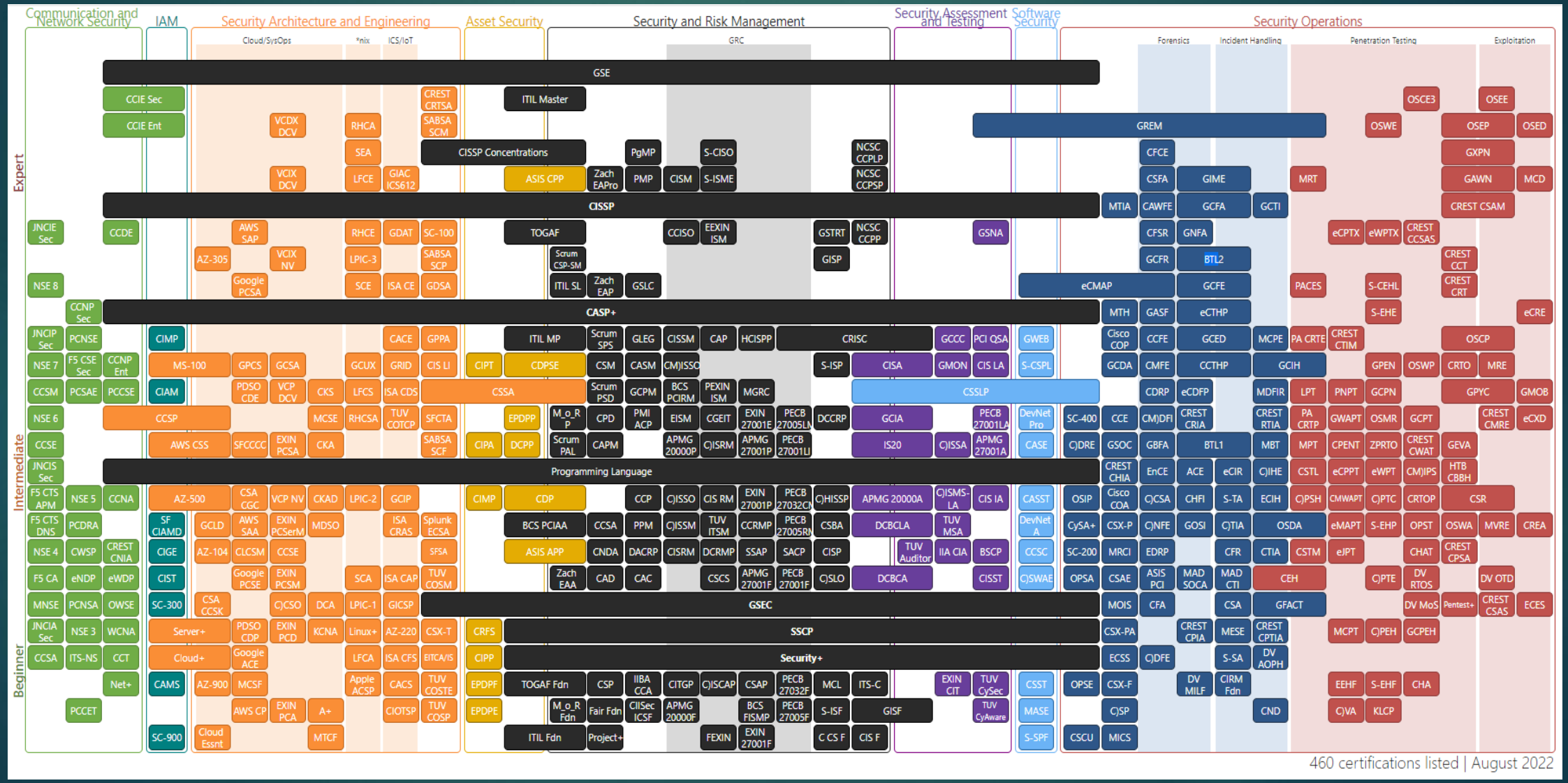
- Current Role
  - Senior Threat Hunter, M&T Bank
    - Vice President
  - CISSP, MS Azure Fundamentals, Network+, Security+ certified
- Previous roles
  - 2.5 years - Risk process technical specialist, M&T
  - 2.5 years - Security Engineer, Seneca Gaming
  - 1 year - IT support technician, Seneca Gaming
- Personal
  - Graduated Buffalo State College class of 2015
    - B.S. Computer Information Systems
    - B.A. Television/Film arts
    - Minor, Philosophy
  - InfraGard Buffalo and Technology advisory board member for the town of Grand Island
  - Amateur boxer out of Casal's boxing club
  - Cybersecurity/Information Security nerd

My Career

- Started out on IT support working overnights
  - Learned troubleshooting hardware, software, networking, systems, DBA, etc.
  - Was very interested in cybersecurity, asked to shadow the ISA (Information Security and Assurance group) after my normal Midnight to 8am shift
  - Assisted on overnight/off hours upgrades such as Firewall upgrades, Content filter upgrades, etc.
- Transitioned to Security Engineering after obtaining **Network+ and Security+**
  - Learned about anti-virus software, firewalls, content filters, SIEM rules, incident response, identity and access management, encryption, etc.
- Joined M&T Bank as a Cybersecurity Risk Process Technical Specialist
  - Designing, automating, and building more efficient processes in vulnerability risk management
  - Less hands on, more of a hybrid between architecture/design, project management, risk management
  - Earned **CISSP and Azure Fundamentals** while on this team
- Became a Threat Hunter after missing the hands-on stuff
  - Staying ahead of adversaries
  - Building defenses with intel and detection engineering
  - Thinking of new protection means
  - Took first ever SANS course **(Non-certification!)**

Ultimate Security Roadmap

- https://pauljerimy.com/security-certification-roadmap/



Certifications

Beginner Certifications

- **CompTIA (https://www.comptia.org/)**
  - No experience necessary
  - Relatively cheap to pay for out of pocket ($200+), cheaper maintenance fees
  - CompTIA requires 3-year recertification with CEUs (Continuing education units)
  - Range of various subjects (networking, security, pentesting, Linux, etc.)
  - Stackable for extra titles

- **Microsoft/Google/Amazon/Vendors**
  - No experience necessary
  - Relatively cheap to pay for out of pocket ($50+)
  - Microsoft Cloud certifications such as Azure Fundamentals, AWS are in high demand
  - Range of various subjects (Cloud, developer, operations, etc.)

Certifications

Advanced (theory based) Certifications

- These are highly desirable certifications due to the experience necessary to obtain them. Typically seen more on mid-level+ job postings

- **(ISC)² (https://www.isc2.org/)**
  - Need to have years of 'real world' experience to obtain full certification. Pass an exam and prove experience to be fully certified
  - Expensive to take exams ($700+), and expensive maintenance fees
  - CISSP requires 5 years of cumulative experience in two of eight domains of the CBK
  - Requires 120 hours of Continuing education credits over three years
- **ISACA (https://www.isaca.org/)**
  - Certifications are more in the cybersecurity risk, incident handling, and governance domains
  - Can be expensive to take exams ($575/member, $760 non-member), but cheaper maintenance fees ($45/yr. member/$85 non-member)
  - Certifications typically require 3 years of cumulative paid experience in two of four domains of the CBK

Certifications

- **“Hands on”/practical Certifications**
  - Typically seen needed for pentesters, web app testers, malware analysis
  - Ones listed below are typically cheaper and great for junior to mid-level job postings

- **eLearnSecurity (https://elearnsecurity.com/)**
  - Several entry to more advanced practical certifications

- **TCM Security -- PNPT (Practical Network Penetration Tester)**
  - https://tcm-sec.com/
  - Relatively cheap for training and testing ($200-$400)
  - Up and coming, slowly becoming more popular in job postings

Certifications

- **Advanced "Hands on"/practical Certification$**
  - Seen a lot more with mid to senior level job postings
- **Offensive Security (https://www.offensive-security.com/)**
  - Need to be hands on knowledgeable in systems, exploits, penetration testing
  - Can be expensive ($1000+ for labs and examination)
  - OSCP is most notable
- **SANS/GIAC Certifications (https://www.sans.org/)**
  - Super expensive (offer 'scholarship'/student proctoring to discount courses
  - Offer practical and non-practical exams
  - Courses typically run $4-10k
  - High quality, seen often on job postings

Debates as old as time

- Certifications versus Experience
- Paying out of pocket versus Employer paid
- Degrees versus Certifications
- How do I know this certification is worth it?
- Bootcamps vs self-study

Questions?

HTTPS://WWW.LINKEDIN.COM/IN/TAYLORANNEKAUFMAN/

^PLEASE INCLUDE SOME REFERENCE TO HACKERS IN HEELS WHEN SENDING AN INVITE