FROM HELP DESK TO ADVANCED THREAT HUNTER

Career talk and progression with:

Taylor Kaufman, CISSP

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
- Certifications 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
  - Advanced Threat Hunter, M&T Bank
    - Assistant 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

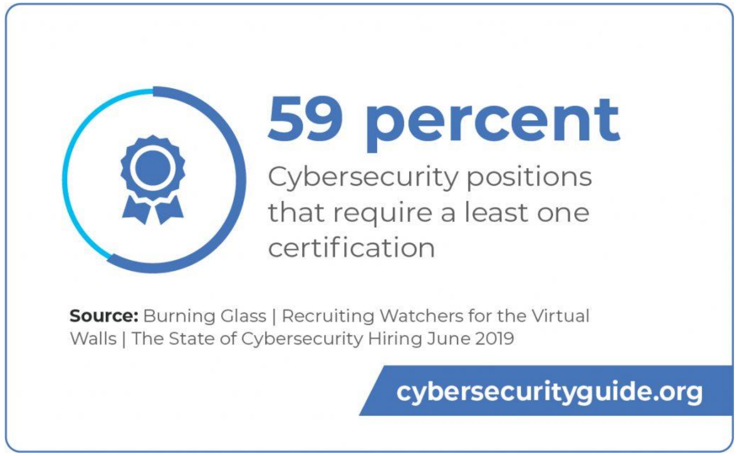
LET'S GET INTERACTIVE!

- Please go to:
- www.menti.com
- Enter code 9753 0155
- Make sure to keep this open for Q&A at the end of the presentation!

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
  - Designing new processes and procedures for new emerging technologies.
  - Less hands on, more of a hybrid between architecture/design, project management, risk management

CERTIFICATIONS



59 percent

Cybersecurity positions that require a least one certification

Source: Burning Glass | Recruiting Watchers for the Virtual Walls | The State of Cybersecurity Hiring June 2019

cybersecurityguide.org

Beginner Certifications

- **CompTIA**
  - 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**
  - 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

CISSP Certified Information Systems Security Professional

Advanced Certifications

- All of these are highly desirable certifications due to the experience necessary to obtain them

- **(ISC)^2**
  - 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 ($120/yr)
  - 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
- **TCM Security**
  - PNPT – Practical Network Penetration Tester
  - 'Real world' certification. Perform a penetration test against a network and present an after action report like you would to a client
  - Exam with training ($399), stand alone exam ($299)
  - Always running sales on their courses. Relatively cheap compared to other practical examinations
- **Offensive Security**
  - Need to be hands on knowledgeable in systems, exploits, penetration testing
  - Can be expensive ($1000+ for labs and examination)
  - OSCP is most notable

THEN I BECAME A THREAT HUNTER…

THREAT HUNTING CAREER

- What is a threat hunter?
  - Threat hunters identify advanced threats, and then track and mitigate them before organizational IT systems are attacked.
- A threat hunter continuously detects, analyzes and combats advanced threats. The job role includes detecting vulnerabilities and mitigating the associated cybersecurity risk before it affects the organization.
- A threat hunter might be tasked with the following:
  - Search for cyberthreats and risks hiding inside the data before attacks occur
  - Gather as much information on threat behavior, goals and methods as possible
  - Organize and analyze the collected data to determine trends in the security environment of the organization
  - Make predictions for the future and eliminate the current vulnerabilities

THREAT HUNTING

- What makes a good threat hunter?
  - Wide range of knowledge including (but not limited to):
    - Networking
    - Systems and OS
    - Applications and APIs
    - Programming and reversing
    - New technologies/IoT/Cloud
    - Security design
    - Pentesting
    - Understanding Log formats, regex, and correlating data
    - Legal risks, incident response/management
- Adversaries have the advantage, its our job to head them off through use of intel gathering and environmental knowledge
- Most importantly, Threat hunters are creative problems solvers!

UNITED STATES

5 MOST-ATTACKED COUNTRY

OAS	33912
ODS	48426
MAV	486
WAV	20205
IDS	86957
VUL	2557
KAS	46098
BAD	2

Detections discovered since 00:00 GMT

More details

735771 979389 33679 380444 1542878 17931 782887 205

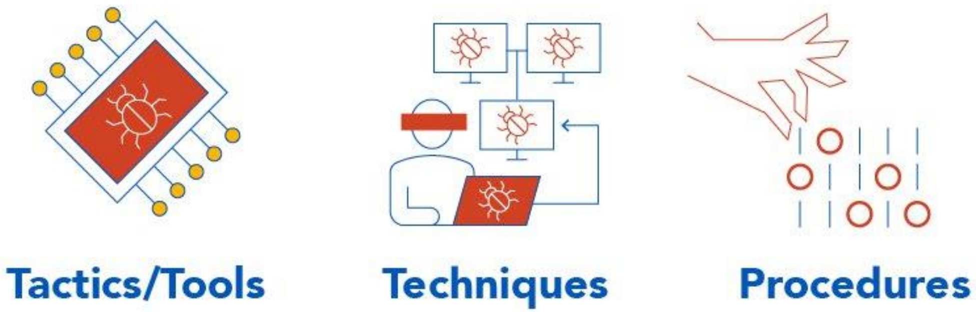
REAL LIFE SCENARIO AS A THREAT HUNTER

- RANSOMWARE:
- March 12th 2021 Buffalo public school systems suffered a ransomware attack
- The average cost of a ransomware attack in 2021 was 4.62 MILLION dollars
- Average cost of a data breach cost in 2021 was 4.24 MILLION dollars
- Cybercrime to cost the world 10.5 TRILLION dollars by 2025

- How to tackle the problem as a threat hunter:
  - Think like an adversary, what is my target? Money? Defacement?
  - If I were to attack my target, how would I approach that?
  - After ID'ing typical approaches though intel and actions learned, figure out what my current defenses are.
  - ID any possible gaps in automated alerting/defenses and create new alerts based off intel
  - Test theories (in a safe environment and safe manner) to generate possible behavior indicators in logs and test newly designed defenses
  - Hunt through history for possible indicators of compromise

THREAT HUNTERS
CANNOT AFFORD TO FALL BEHIND

- Industry is ever evolving, and quickly. Threat hunters NEED to keep up with industry best practices, new technologies that business might implement, and stay on top of new TTPs (Tactics, Techniques, and Procedures)



- How I keep my skills sharp:
  - Tryhackme.com
  - Pluralsight
  - Microsoft, Amazon, Google
  - Webinars, etc.: SANS, TrustedSec, etc.
  - Capture the Flag events/sites:
    - Hackthebox, overthewire, MetaCTF
    - SANS holiday hack challenge
  - Social media: Twitter, Reddit, etc.
  - Top cyber investigative groups like Google project 0, anti-virus vendors, Bug bounty programs, etc.
  - Lots of research!

PLAY TO YOUR STRENGTHS

- For students who show an interest in technology careers but aren't quite sure:
  - Like art and design? Graphic design, UX/UI designer
  - Like science? Data engineering, quantum computing
  - Like math? Blockchain and crypto technologies
  - Like social networking? Threat analyst and OSINT (open source intelligence gathering)
  - Thinking about law? Compliance and regulation, risk management and privacy
  - Better at taking things apart? Forensics and reverse engineering malware
  - Architecture? You can architect networks and secure design for businesses
  - Good at finding problems? QA tester
  - Like programming? Learn how to securely code

  - I have people on my team with physics degrees, people who drove gunner tanks for the army, people with English degrees, etc. Technology and cyber folks are a melting pot of backgrounds.

QUESTIONS?

WWW.MENTI.COM

ENTER CODE 9753 0155

- Taylorannekaufman@gmail.com
- https://www.linkedin.com/in/taylorannekaufman/