UPPING YOUR CYBER SKILLS

Inspiring a love of cybersecurity:

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 and sites 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!**

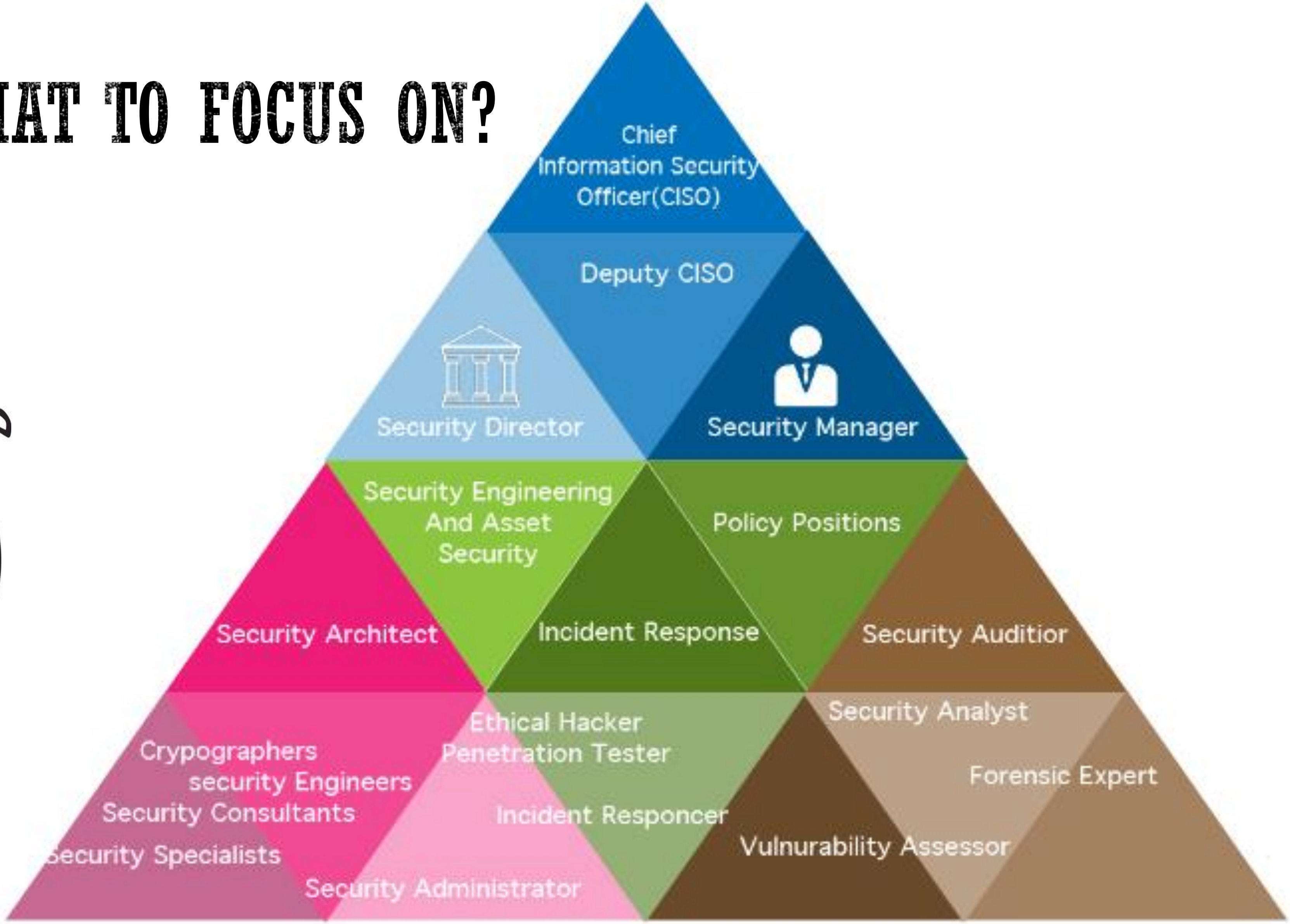
ABOUT ME

- 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

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
- 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

HOW DO I DECIDE WHAT TO FOCUS ON?



Chief Information Security Officer(CISO)

Deputy CISO

Security Director

Security Manager

Security Engineering And Asset Security

Policy Positions

Security Architect

Incident Response

Security Auditior

Crypographers
security Engineers
Security Consultants
Security Specialists

Ethical Hacker
Penetration Tester

Incident Responcer

Security Administrator

Security Analyst

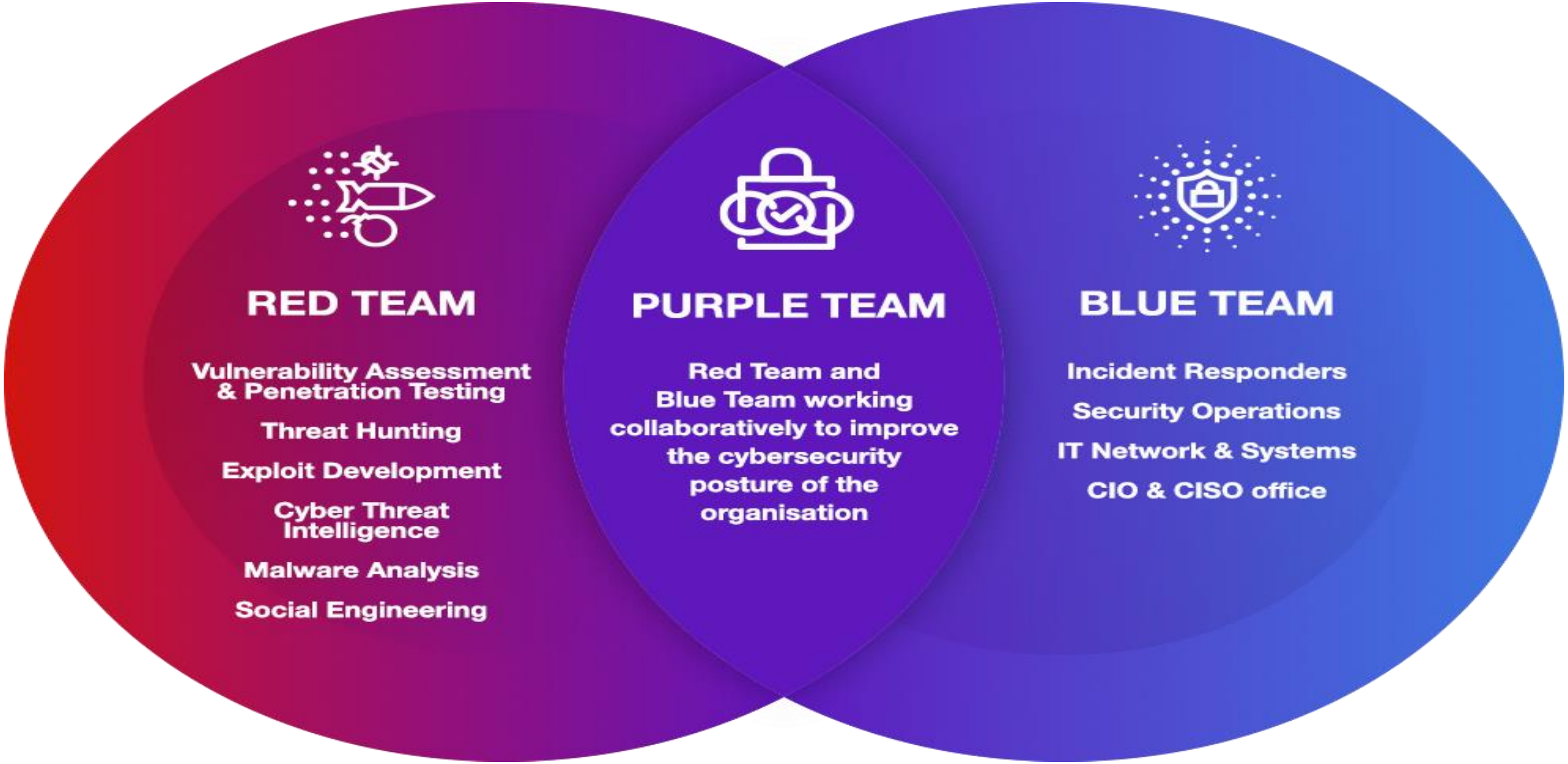
Forensic Expert

Vulnerability Assessor

APPEAL TO STRENGTHS

- For students who show an interest in technology or cyber 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

OFFENSIVE SECURITY VS DEFENSIVE SECURITY VS HYBRID SECURITY



RED TEAM

Vulnerability Assessment & Penetration Testing

Threat Hunting

Exploit Development

Cyber Threat Intelligence

Malware Analysis

Social Engineering

PURPLE TEAM

Red Team and Blue Team working collaboratively to improve the cybersecurity posture of the organisation

BLUE TEAM

Incident Responders

Security Operations

IT Network & Systems

CIO & CISO office

HOW I KEEP MY SKILLS SHARP

- How I keep my skills sharp:
  - Tryhackme.com
  - Pluralsight, cybrary, itprotv
  - Codeacademy
  - Microsoft, Amazon, Google, security/tech vendors (ibm, palo alto, etc.)
  - Webinars, etc.: SANS, TrustedSec, TCM security, etc.
  - Capture the Flag events/sites:
    - Hackthebox, overthewire, MetaCTF
    - SANS holiday hack challenge, PicoCTF
  - Social media: Twitter, Reddit, YouTube, etc.
  - ThreatGen Red Vs Blue, rangeforce
  - Top cyber investigative groups like Google project 0, anti-virus vendors, Bug bounty programs, etc.
  - Lots of research and reading!

LET'S LOOK AT SOME OF THESE RESOURCES…

COMPETITIONS – CTF 101

- CTF (Capture the Flag) is a kind of information security competition that challenges contestants to solve a variety of tasks to find a specific piece of text that may be hidden on the server or behind a webpage. This goal is called the flag.
- Example of a typical flag format: CTF{Th1s1s@Fl@g!!kl23$#s}
- The very first cyber security CTF developed and hosted was in 1996 at DEFCON in Las Vegas, Nevada.
- Can be held on site or online and can be played as an individual or in teams.
- Major events such as Google CTF, Defcon CTF, HITB, etc. all offer major monetary prizes and exposure for security professionals who compete.

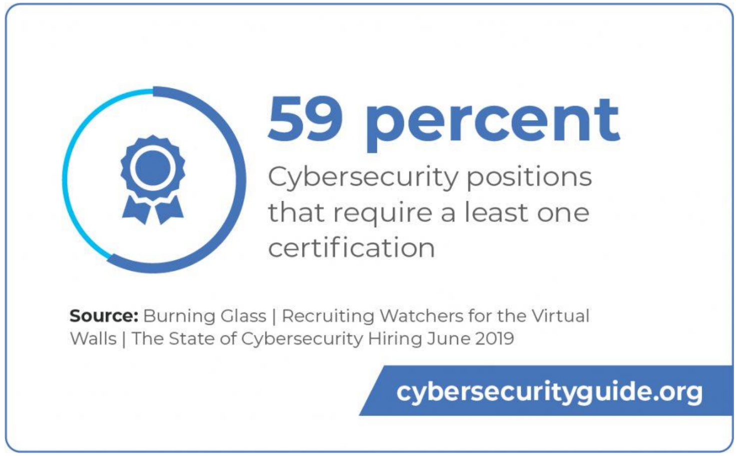
Capture the Flag:
It's a game for hack..
I mean security professionals

WHERE DO I START FOR CTFS?

- Commonly used tools:
  - OS such as BlackArch, Parrot, or Kali Linux
  - Binwalk – extract and analyze files
  - Burp suite – web pent tools
  - Stegsolve – for finding anything hidden within images, etc. (steganography)
  - IDA – reverse engineering
  - COMMAND LINE!!!
  - Big breakdown guide here: https://github.com/apsdehal/awesome-ctf
  - Owning a dark hoodie never hurt

- Entry level practice sites:
  - PicoCTF – originally designed for middle schoolers and high schoolers, you don't need to download any tools. All done through web.
  - CTFlearn.com – various collected challenges aimed towards newcomers
  - Overthewire.org/wargames and hackthebox – connect to games via SSH (like putty) and use tools on your own machine to try these challenges
    - Please note: there are a lot of established write ups for these challenges. If you wish to work through them yourselves, make sure to avoid youtube or git repositories with them

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 Cyber/Tech 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.)

WHAT ABOUT PENTEST TOOLS?

- https://shop.hak5.org/
  - one of the few sites I trust for COTS pentesting tools
- Lockpicking sets
  - Again, why ethics are so important
- Flipper Zero
  - https://flipperzero.one/

QUESTIONS?

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