TrustedSec

Finding Your Home in Infosec

To Specialize or Not

With: Adam Compton

Date: May 12, 2023

Presentation Overview

- Diverse landscape of information security
- Personal stories and experiences
- Audience engagement and Q&A session

Target Audience and Goals

For those just getting into infosec and looking for a change

- Identify a potential niche for your skills and interests
- Share valuable insights from real-life experiences
- Hopefully encourage audience engagement

Me?

Adam Compton

Principal Security Consultant

Over my career I have been a programmer, researcher, instructor, professional pen tester, father, husband, and farmer.

I have nearly two decades of experience in the Information Security field performing programming, network security, incident response, security assessment, and penetration testing.

Importance of Choosing the Right Infosec Path

- Increased job satisfaction
- Better utilization of skills and passions
- Greater opportunities for growth and development

Diverse Landscape of Information Security

- Penetration Testing/Pentesting
- Red Teaming
- Incident Response
- Defensive Security/Blue Teaming
- Research/Development

Pentesting

Simulates either an active attack against external company resources or an active attacker which is already internal to the network.

Key Responsibilities:

- OSINT
- Misconfiguration/Vulnerability detection and exploitation
- Manual and automated testing
- Reporting

Pentesting Skills and Certifications

Essential Skills:

- Curiosity/Determination
- Network/Protocol/Communication protocols
- Accuracy and Integrity
- **Scripting

Popular/Useful Certs:

- CEH
- OSCP
- GPEN

Red Teaming

Red Teaming is a goal-oriented, offensive security assessment designed to test an organization’s preventative and detective controls by simulating a determined, skilled intruder

Key Responsibilities:

- Expectation management
- Significant “soft” skills.
- Full project leadership
  - including presentations to a variety of audiences
- TS red teams are typically full scope

Red Teaming Skills and Certifications

Key Skills:

- Coding - Python/C#/C
- Standard penetration testing skills and familiarity
- Curiosity / Persistence / Fearlessness.
- Red teaming is much slower than pentesting.
- Integrity and humility.

Popular/Useful Certs:

- OSCP
- OSEP
- CRTO

Incident Response

Incident Response is the process of detecting, analyzing, and responding to security incidents in an organization. It is reactive - meaning it happens after something has occurred.

The goal of any IR engagement is to find out what happened, stop the attacker from continued operations, and recover the organization back to normal operations.

Key Responsibilities:

- Forensic analysis of systems and logs
- Familiarity with attacks, how to detect them, and how to respond to them
- Containment, eradication, and recovery recommendations
- Translating "tech speak" to key decision makers (e.g. C-level)
- Incident management

Incident Response Skills and Certifications

Key Skills:

- Ability to stay calm under pressure
- Computer and network forensics
- IR containment, eradication, and recovery strategies
- Communications
- Teamwork and collaboration

Popular/Useful Certs:

- Any of the SANS forensics/IR certs
- CISA.gov (US CERT) certs
  - (https://www.cisa.gov/resources-tools/programs/Incident-Response-Training)

Research/Development

Provide a strategic advantage by providing tooling and knowledge that are a differentiator in an ever more complex and challenging market.

Key Responsibilities:

- Tool Development
- Exploit Research/Development
- Research multiple technologies for better understanding
    - useful for training and development of new TTPs

Key Skills:

- Critical thinking
- Have developed autodidact skills
    - ability to teach yourself about different technologies
- Have development skills
    - ability to test and develop theories
- Flexibility across languages
    - not bound or obsessed on a single one.

Defensive Security/Blue Teaming

Defensive Security often known by its nomenclature "Blue Team," is generally thought of encompassing such areas of information security: Intrusion Analysis/SOC, Threat Hunting, and (DF)IR

The primary goal of the Blue Team, is to be the "eyes and ears" of an organization by detecting, responding, and triaging malicious activity effecting the organization's information assets.

Having a basic understanding of the organization's mission, business, operations, assets, and what are they trying to protect and who may be targeting the organization are key.

Defensive Security Skills

Key Skills:

- Network traffic analysis
- Detection rule writing (query languages, sigma, yara, etc)
- Knowledge of OS internals
- Ability to reverse engineer malware and performing analysis
- Performing incident response
- Memory forensics

My Infosec Journey

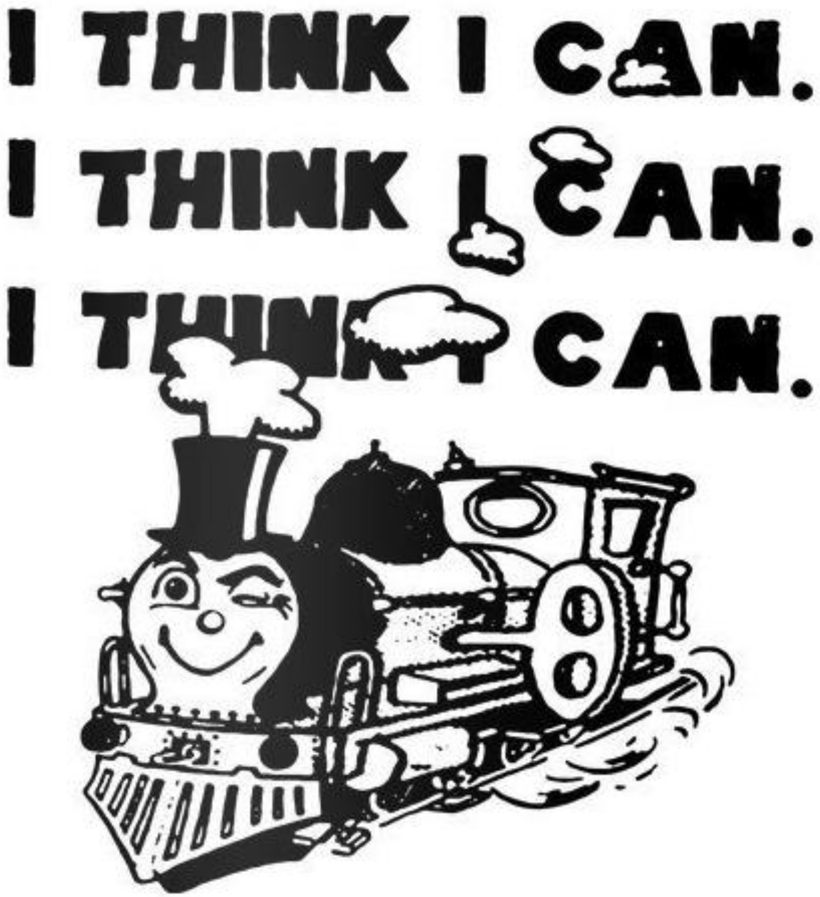
Time to talk about me:

Key Milestones:

- Got a Computer
- Became a co-op at the DoD
- Got a job pentesting mostly by accident
- Moved jobs (several "5" times)

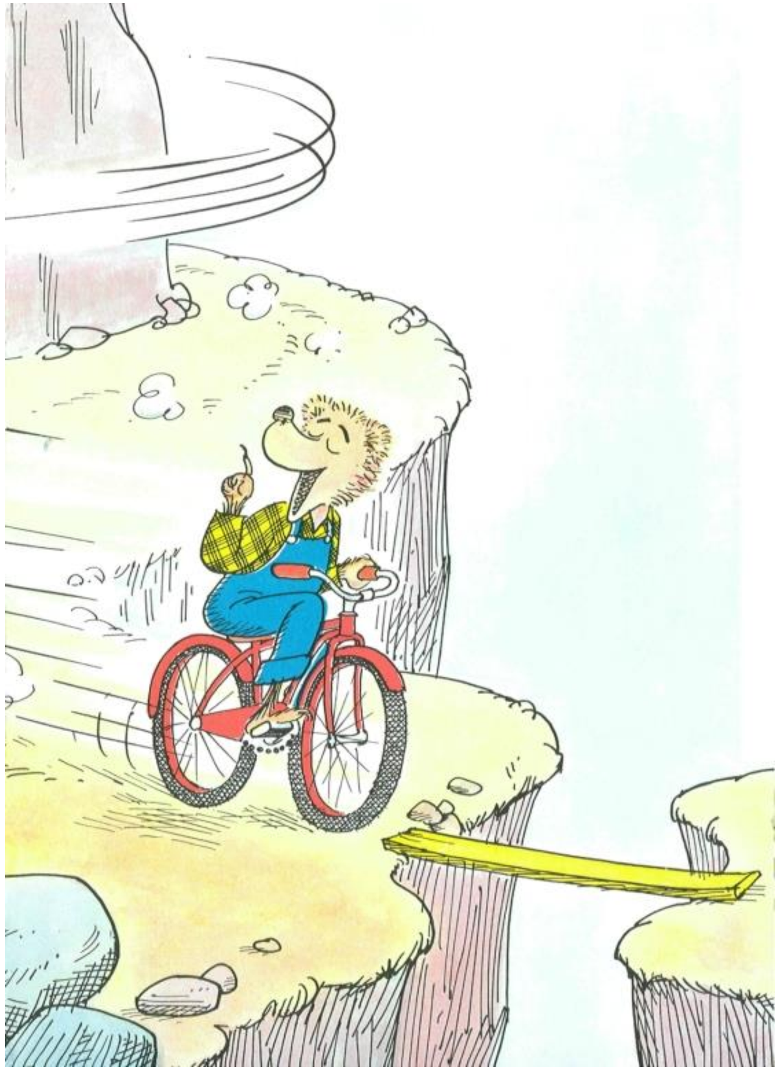
Challenges and Overcoming Them

- Ever changing world of InfoSec/consulting
- Diversifying/Focusing my skill set
- Dissecting job postings/descriptions
- Learning balance and finding the happy medium

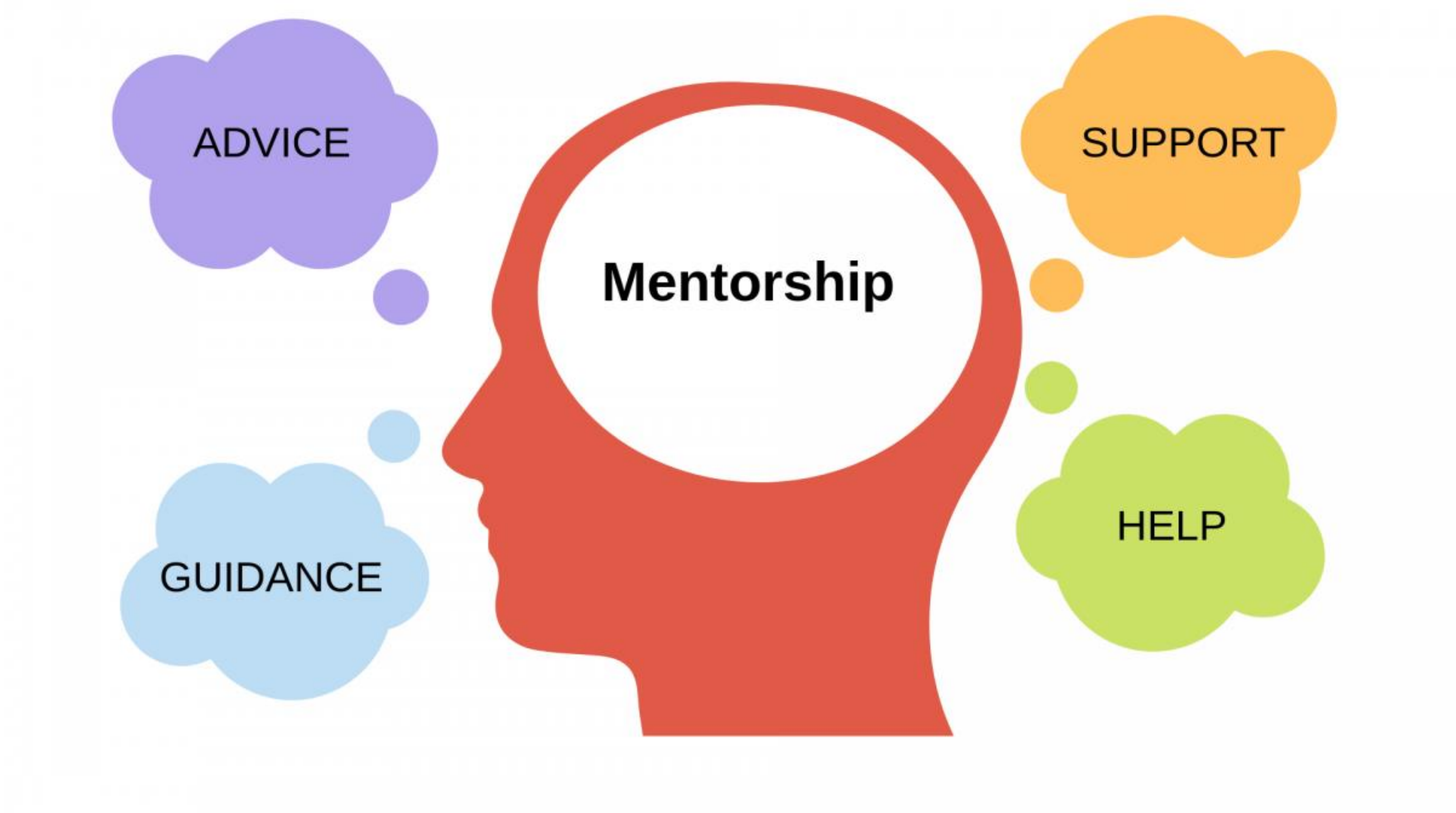


Lessons Learned and Advice

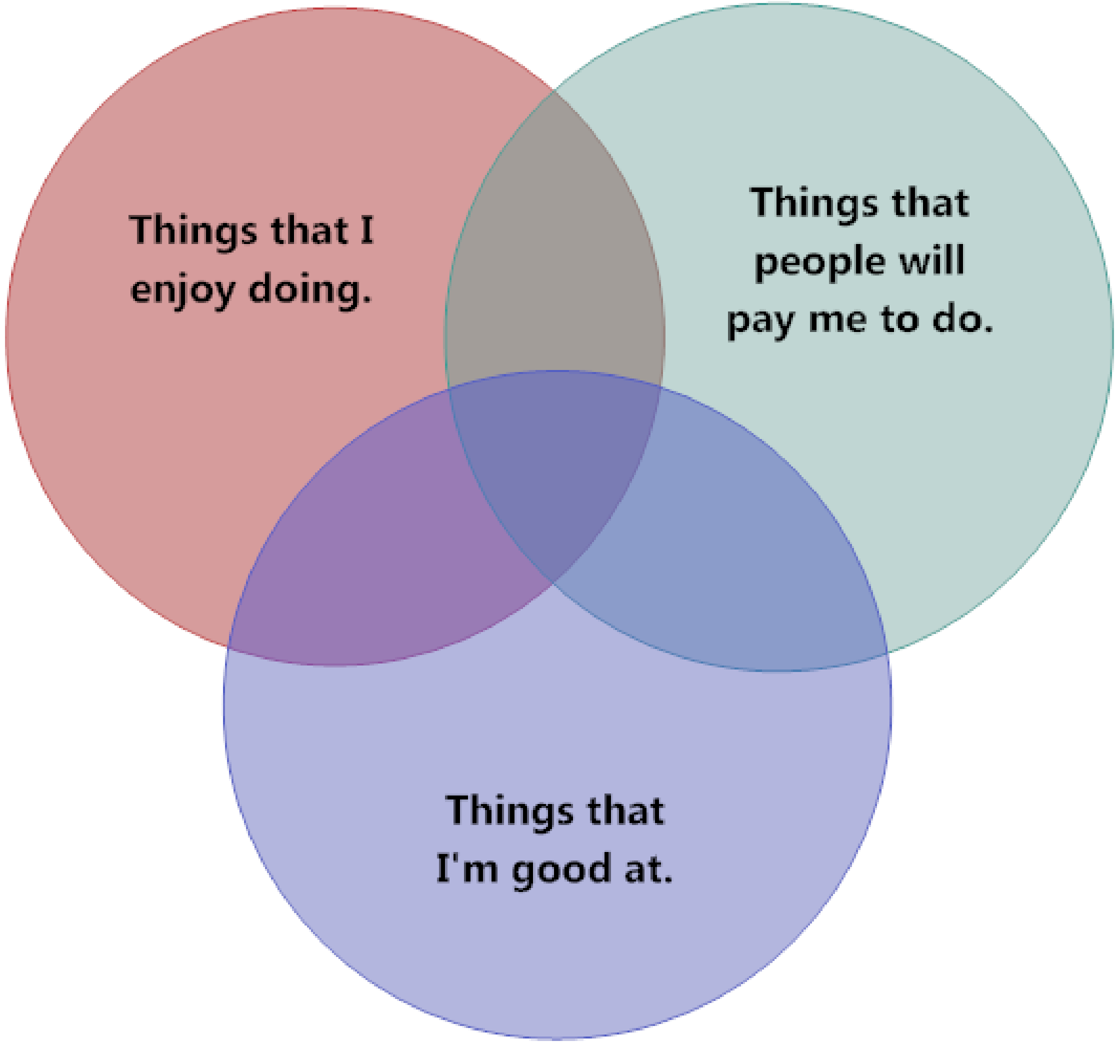
- Stay open to new possibilities/opportunities
- Try to not become complacent
- Watch out for burn-out
- No one is good at everything



Networking and Mentorship



Identifying Personal Skills, Interests, and Passions



Things that I enjoy doing.

Things that people will pay me to do.

Things that I'm good at.

Path Forward

Exploring Resources and Opportunities

- Online resources: blogs, discord, webinars
- Local infosec meetups and conferences
- Training and educational programs

Setting Goals and Creating an Action Plan

- Importance of setting realistic and achievable goals

Recap of Key Points

SUMMARY

- Many career paths in InfoSec
- Your path will be different from everyone else's and that is ok

Q&A Session

@tatanus

www.hillbillystorytime.com

www.youtube.com/hillbillystorytime

adam.compton@gmail.com

adam.compton@trustedsec.com