LET'S TALK ABOUT BRUNO:
THE REALITY OF THE CYBERSECURITY TALENT SHORTAGE

Michael Miller

AGENDA

- Introductions
- The Problem(s)
- Issues Deep Dives
- What Can We Do
  - As Managers
  - As Job Seekers
- Summary

$>WHOAMI

Experience

- Cybersecurity Platform Engineering Manager at Cardinal Health
- Previously Global Cybersecurity Manager at Cooper Tire
- IT/Cybersecurity for 11+ years in a variety of industries
- Worked with companies ranging in size from <$1M to >$100B

Education

- BS Cybersecurity & Information Assurance from WGU
  AAB Network Administration & Computer Programming from NSCC
- CCSP, SSCP, CEH, ECES, CySA+, Security+, Network+, A+, Project+, CCFA, CCFR

Personal

- Spending time with family, grilling/smoking, working in home lab, and traveling
- Participate in InfraGard, ISSA, (ISC)2, Advisory Board for NSCC, CAMO at NSCC, Adjunct Teacher at NSCC

WHO ARE YOU?

- InfoSec Professionals?
- Hiring Managers?
- Industry Job Seekers?
- Students?

THE PROBLEM(S)

A DOUBLE-EDGED SWORD

Hiring Managers

- Issues finding qualified talent
- Disconnect between HR and needs
- Unsure of team requirements
- Limited number of positions
- Need for senior skillsets
- Unrealistic candidate expectations

Job Seekers

- Issues getting interviews
- Issues getting hired
- Lack of entry level positions
- Can’t get job without experience
- Unrealistic job descriptions

ISSUES DEEP DIVE

LACK OF ENTRY-LEVEL POSITIONS

- Lots of internships, lots of mid to senior roles, but not very many true entry-level roles
- Most cybersecurity roles have the expectation of underlying IT knowledge which leads to many considering cybersecurity to not have “entry-level” roles
- Many roles posted as “entry-level” have unrealistic requirements either in the form of years of experience or certifications
- This is often because of salary limitations for hiring companies

UNREALISTIC EXPECTATIONS - COMPANIES

- Entry-level positions expecting many years of experience
- Entry-level positions expecting a masters degree
- Entry-level positions expecting a **CISSP**
- Senior-level experience requirements paying < $100k
- Expecting security folks to know **everything**
- Refusing to allow remote work where it is possible
- Poor work/life balance

Required Technical and Professional Expertise

- **Minimum 12+ years' experience in Kubernetes administration and management**
- Hands-on experience on setting up Kubernetes platform, deploying microservices and other web applications, and managing secure secrets along with container orchestration using Kubernetes

Kubernetes

Computer application

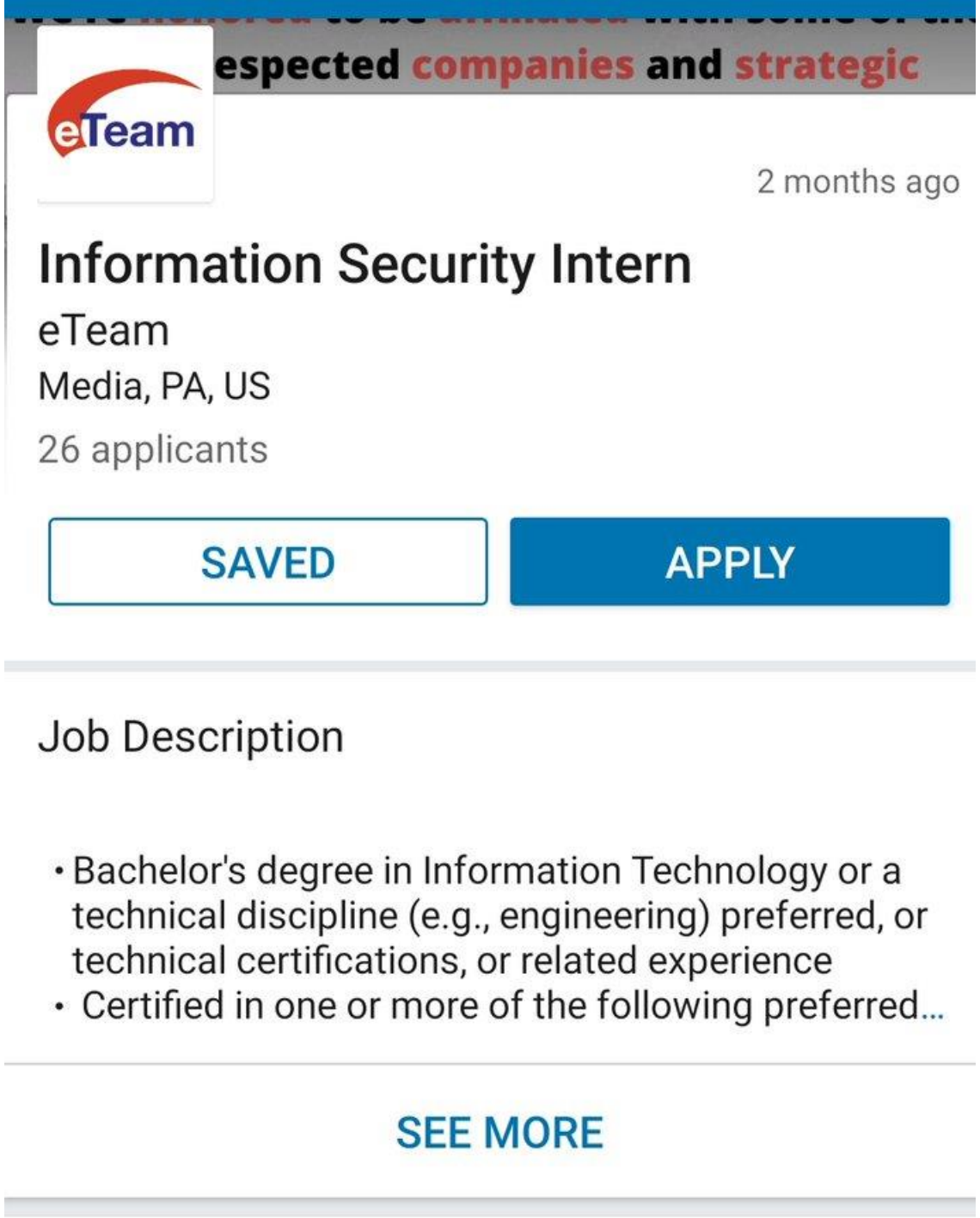
Kubernetes is an open-source container-orchestration system for automating computer application deployment, scaling, and management. It was originally designed by Google and is now maintained by the Cloud Native Computing Foundation. Wikipedia

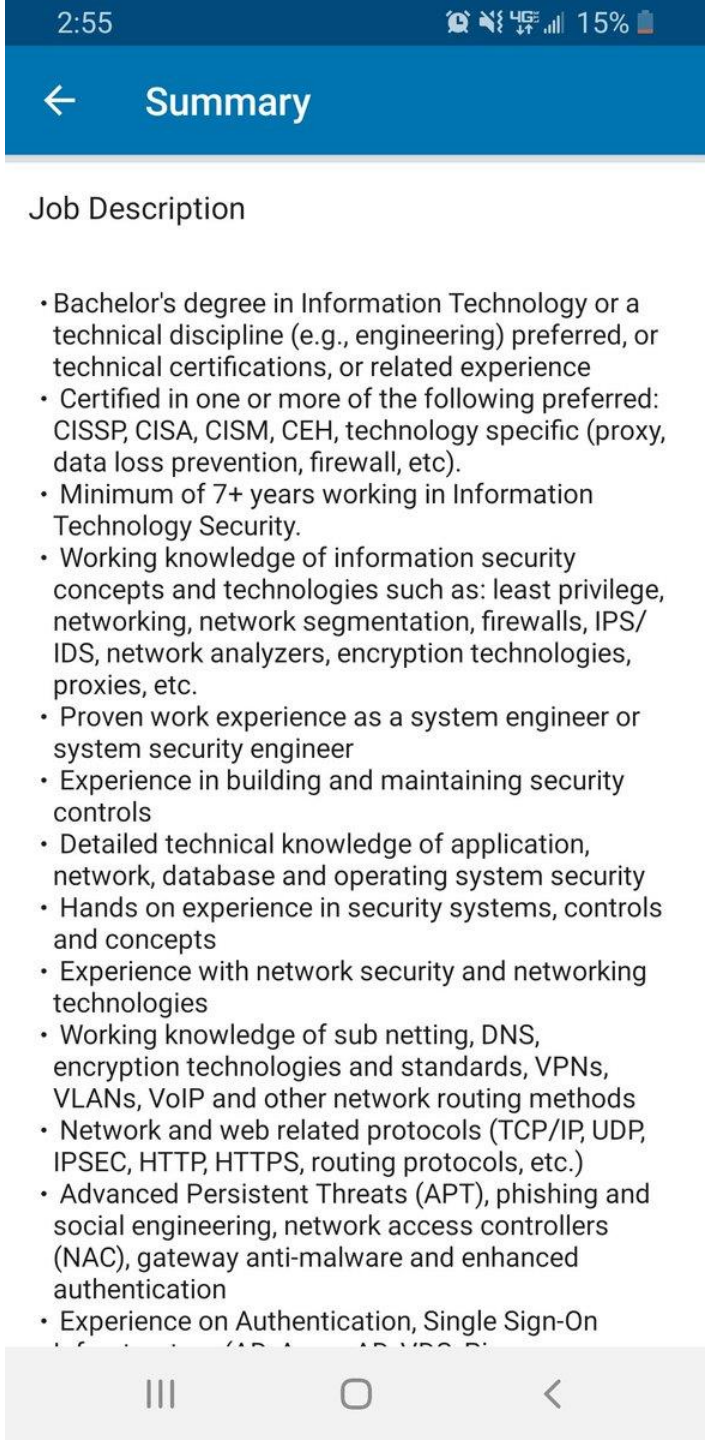
Written in: Go

Developed by: Cloud Native Computing Foundation

Initial release: 7 June 2014; 6 years ago

* Thanks to Ryan Fennell for finding this again for me


espected companies and strategic
eTeam
2 months ago
Information Security Intern
eTeam
Media, PA, US
26 applicants
SAVED
APPLY
Job Description
• Bachelor's degree in Information Technology or a technical discipline (e.g., engineering) preferred, or technical certifications, or related experience
• Certified in one or more of the following preferred...
SEE MORE


2:55
15%
Summary
Job Description
• Bachelor's degree in Information Technology or a technical discipline (e.g., engineering) preferred, or technical certifications, or related experience
• Certified in one or more of the following preferred: CISSP, CISA, CISM, CEH, technology specific (proxy, data loss prevention, firewall, etc).
• Minimum of 7+ years working in Information Technology Security.
• Working knowledge of information security concepts and technologies such as: least privilege, networking, network segmentation, firewalls, IPS/IDS, network analyzers, encryption technologies, proxies, etc.
• Proven work experience as a system engineer or system security engineer
• Experience in building and maintaining security controls
• Detailed technical knowledge of application, network, database and operating system security
• Hands on experience in security systems, controls and concepts
• Experience with network security and networking technologies
• Working knowledge of sub netting, DNS, encryption technologies and standards, VPNs, VLANs, VoIP and other network routing methods
• Network and web related protocols (TCP/IP, UDP, IPSEC, HTTP, HTTPS, routing protocols, etc.)
• Advanced Persistent Threats (APT), phishing and social engineering, network access controllers (NAC), gateway anti-malware and enhanced authentication
• Experience on Authentication, Single Sign-On

Cyber Security Engineer - Entry Level

El Segundo, CA 90245

Urgently hiring

Job Type
Full-time

Qualifications

- Master's (Preferred)
- Linux: 2 years (Preferred)
- Information Security: 2 years (Pref
- CISSP (Preferred)
- US work authorization (Preferred)

License/Certification:

- CISSP (Preferred)

Willingness To Travel:

- 25% (Preferred)

Work Location:

- One location

Work Remotely:

- No

Responsibilities

· Deliver of efficient, maintainable, robust and reusa

· Manage critical infrastructure hosting Cloud Native and On-Prem custom hardware

· Install, integrate, and deploy enterprise Cyber Secu environments

· Gather, link and analyze data from various sources

· Review analytics results, investigate incidents, anor

· Understand cyber security and technology product different data sources for cyber security incident an

· Create and work closely with engineering team for

· Troubleshooting security and network problems

· Daily administrative tasks, reporting, and commun departments in the organization.

· Project documentation including technical requirer run-book

· Develop prototypes of system designs and work wi technical support and other IT areas as appropriate implementation processes

· Work with multiple project teams with competing c

Education & Experience

· Bachelor's Degree in Computer Science, Engineering, degree or equivalent and two years of work experience or Masters in Computer Science / Engineering

· CISSP or similar security certification is a plus

· Experience with the following technologies: Linux, Win 10, Win 7, XP, Vista, Win Server 2003, Active Directory, SIEM (Splunk, QRadar, ArcSight), Logstash, Hadoop, MySQL, CRATE, Netflow, PCAP, Syslog, TCP/IP, DNS, and DHCP, IDS / IPS.

· Experience with Firewalls (functionality and maintenance), Office 365 Security, VSX, and Endpoint Security.

· Proficiency in Python, C++, Java, Ruby, Node, Go, and/or Power Shell.

· Advanced understanding of common network services (web, mail, FTP, etc), network vulnerabilities, and network attack patterns

Secure https://www.indeed.com/m/viewjob?jk=a8c7aa6d289e7f45&from=serp

Application Security Engineer

Application Security Engineer – Digital Trust
Capital One (yes, the "what's in your wallet?" company!) is rethinking the way the world approaches banking. We're experimenting, innovating, and delivering breakthrough experiences for 65 million customers. We love to be curious, to dream, and ask "What if?" Oh, and we love to write code , and not to brag, but we're also a great place to work!

As a member of a technology team working on an innovative digital product under the Capital One Technology Fellows Program, the Application Security Engineer will join a team of application security professionals focused on ensuring data safety and system security for an innovative, new digital product. The Application Security Engineer will work closely with agile software development teams building the product as well as the security and compliance engineers from the company-wide units to design, automate and execute security threat modeling, code reviews, and vulnerability testing. Security for us is not an afterthought but an integral part of the engineering process. As such, application security engineering team is involved at each stage of the application built-out and has a significant voice in the architecture and implementation of the solution.

Responsibilities can include, but are not limited to:
Deliver relevant application security training and mentorship to development teams.
Participate in and lead solution design of critical parts of the application, especially the ones related to data encryption and storage at rest and in transit.
Identify emerging vulnerabilities, risks, and threats during design iterations and provide appropriate countermeasures and backlog security stories
Review and test open source and proprietary code
Test new features and builds during agile sprints
Prevent security issues in production
Monitor developments within the application security industry to ensure internal policies, procedures, tools, and training reflect current trends and methods such as those published by OWASP
Build custom tools, scripts, libraries, and platforms to test security and improve security.
Collaborate with other information security teams in the evaluation, development, implementation, communication, operation, monitoring and maintenance of security policies and procedures to promote a secure and innovative environment

Basic Qualifications
Bachelor's degree or military experience
At least 3 years of professional software development experience
At least 5 years of security program management experience, covering activities like penetration testing, static analysis, and dynamic testing policies and procedures.
At least 5 years of experience evaluating and addressing security vulnerabilities with iOS (Swift, Objective-C), Android (Java) apps and their server side API's.
At least 5 years of experience with mobile app hacking tools.
At least 5 years of experience securing open APIs and web applications over HTTP.
At least 5 years of experience in data encryption and data storage safety at rest and in transit, for large scale applications.
At least 5 years of experience assessing and securing iOS and Android mobile apps
At least 5 years of experience reviewing source code for security and administering large-scale security testing, including various types of penetration testing.
At least 5 years of experience in threat modeling web and mobile applications

Preferred Qualifications
At least 5+ years of experience in securing data storage systems with distributed usage patterns
At least 1+ years of experience with distributed identity systems
At least 1+ years of experience securing microservice architecture systems
At least 1+ years of experience securing highly sensitive systems for the federal government and/or financial institutions
At least 3+ years of experience with security-related NIST, PCI and HIPAA/HITECH provisions.
At least 1+ years of experience with Golang, Node, Java, Objective-C, Swift and Python.
At least 1+ years of experience with CSSLP, CISSP, CEH and OSCP.

What to Expect
The Digital Products Engineering team is responsible for building consumer web and mobile applications. Our award-winning apps enable our 45 million customers to manage their data and finances. The apps are also mobile e-commerce platforms, enabling new customer and account origination.
Protecting our customer's sensitive financial and personal information is our top priority. We are looking for someone to continue to push the state-of-the-art in web and mobile application security and to integrate these solutions into our best-in-class applications. Our goal is to provide the best possible customer experience, and we will settle for nothing less. If Diffie–Hellman key exchange is your thing, and you quote Shannon at dinner parties - then please get in touch with us!

Responsibilities:
Driving and iterating on a web and mobile application security program, working closely with several development teams to integrate security practices into a number of applications throughout the agile development cycle.
Work continuously with product, design, & engineering teams to identify application security requirements as applications continue to grow and evolve.
Grow and provide SME level leadership in iOS and Android mobile client and API security.

UNREALISTIC EXPECTATIONS - CANDIDATES

- Expecting senior-level salary with no experience
- Expecting senior-level roles with no experience
- Thinking a couple week bootcamp makes them qualified for everything
- Expecting huge training budgets

EXPLOITATION OF JOB SEEKERS & INDUSTRY BOOM

- Unfortunately, the shortage of talent has made it easy for companies/groups to take advantage of the booming market and desperate job seekers
- Comes in the form of unrealistic marketing and empty promises
- There are plenty of notorious bootcamps out there that make huge promises, pack of bunch of free information into a few weeks, and take your money
- Some Universities are doing this too…

FORTUNE | EDUCATION ARTICLES CAREER GUIDES RANKINGS MORE

Cybersecurity master's grads are landing $200K-plus pay packages

BY SYDNEY LAKE

November 21, 2022, 12:16 PM

STUDENTS ON THE UNIVERSITY OF CALIFORNIA, BERKELEY CAMPUS IN BERKELEY, CALIFORNIA, US, AS SEEN IN AUGUST 2022. (PHOTOGRAPHER: DAVID PAUL MORRIS—BLOOMBERG/GETTY IMAGES)

- Graduates from top-ranked cybersecurity programs can expect to make six-figure starting salaries **between** $100,000 and $200,000.
- Article refers to a **California based school** listing its program as the No. 1 program in the country
- …which Fortune ranks as having the No. 2 online cybersecurity master's program, graduates make **$112,000 median base salaries** right after graduation, and $126,000 one year post-graduation.
- …reports **mean base salaries for its cybersecurity grads at $77,400**, which is a 44% increase over what they earned prior to enrollment. Fortune ranks Indiana as having the No. 4 cybersecurity master's program in the U.S.

WHAT CAN WE DO

As Hiring Managers

KNOW YOUR TEAM & NEEDS

Skill gaps

- Where are gaps in capabilities
- Focus on what will augment your team

Skill strengths

- Where are your strengths
- Don’t just hire people with the exact same skillsets
- Consider remote positions if you don’t already

COLLABORATE WITH HR

- Get to know your HR team
- Discuss hard company requirements (e.g., education)
- Discuss things you have control of in both the job description and the interview process
- Discuss qualifying and disqualifying questions for the pre-screen
- Take the time to go through a handful of resumes with them

IMPROVE JOB DESCRIPTIONS

- Consider Diversity, Equity, and Inclusion
- If possible, eliminate certain educational **requirements**
- If possible, eliminate years of experience **requirements**
- If possible, eliminate discriminatory language
- Focus on proficiency and level of expertise in skills, frameworks, and technologies
- Don’t forget your OpSec

CYBERSECURITY INFRASTRUCTURE ENGINEER

- Job Responsibilities Include:
  - Implementing and supporting security platforms related to: Cloud Access Security Broker (CASB), automated Internet of Things (IoT)/Operating Technology (OT) asset discovery, advanced anti-malware, network intrusion detection system (NIDS)/network intrusion prevention system (NIPS), web application firewall (WAF), Data Loss Prevention (DLP)
  - Building of Linux servers, dockers, containers, automation in GCP
  - Continuous optimization, tuning and monitoring of platforms
  - Troubleshooting issues affecting internal customers
  - Executing small/medium projects to deploy security platforms into the business to maximize value and enhance security posture
  - Integration of platforms into SIEM, SOAR and/or API's
  - Working closely with Security Incident Response, Purple, Threat Intel teams
  - Onboarding of new security platforms into an operational model from the Security Architecture team
  - Participation in POC/RFP by testing solutions or building test environments
  - Managing Open Source, SaaS, and on-premise platforms

- Job Responsibilities Include:
  - Administrating and supporting various security platforms such as: Endpoint Protection/Endpoint Detection & Response (EPP/EDR), Vulnerability Management systems, Intrusion Detection Systems (HIDS, HIPS, NIDS, & NIPS)
  - Building and managing infrastructure using virtualization and container technologies (primarily Linux)
  - Integrating platforms through APIs
  - Automating processes through scripts and orchestration platforms
  - Continuous optimization, tuning and monitoring of platforms
  - Troubleshooting issues affecting internal customers
  - Executing small/medium projects to deploy security platforms into the business to maximize value and enhance security posture
  - Onboarding of new security platforms into an operational model from the Security Architecture team
  - Participation in POC/RFP by testing solutions or building test environments

CYBERSECURITY INFRASTRUCTURE ENGINEER

- Required
  - Familiarity with implementing and supporting several infrastructure or security platforms to include optimization, troubleshooting and tuning
  - Ability to collaborate with numerous teams and internal customers
  - Development of Build/Run processes to ensure systems are properly maintained and operating effectively
  - Familiarity with the Linux operating system
  - Familiarity with networking principles
  - Familiarity with containerization
- Preferred
  - SIEM, CASB, WAF, NIPS/NIDS or DLP experience a plus
  - Python, BASH, C++ and interfacing with REST API's is a plus
  - Experience with networking, servers, web servers, and firewalls.
  - Experience in Linux, GCP, Dockers/containers and GCP automation is desired.
  - A good working knowledge of security best practices, defense in depth, or MITRE ATT&CK framework. Security experience or certification is a plus.
  - Experience in a large enterprise environment (2000+ users) is a plus

- Required
  - Experience administrating and supporting infrastructure and security platforms
  - Familiarity with the Linux operating system
  - Familiarity with networking principles and technologies
  - Ability to collaborate with numerous teams and internal customers
- Preferred
  - Familiarity working with scripting technologies (Python, Bash, PowerShell) and interfacing with APIs
  - Familiarity with security frameworks (MITRE ATT&CK, NIST CSF, etc.)
  - Familiarity working in cloud technology platforms (GCP, AWS, Azure)
  - Familiarity with containerization technologies (Docker, Kubernetes)
  - Familiarity with Infrastructure as Code (IaC) (Ansible, Terraform)
  - Experience in a large enterprise environment (2000+ users) is a plus

IMPROVE INTERVIEW PROCESS

- Involve your team in the panel interviews
- Create diverse panels (gender, race, culture, experience, etc)
- Focus on questions that allow you to gauge comprehension, critical thinking, and personality as well as skills
- Discuss the expectations of the position, and highlight important things from your team’s culture

NETWORK

- How many of you are looking for a job right now?
    - **Talk to these folks**
- Get involved in local professional groups like BSides, ISSA, and InfraGard

WHAT CAN WE DO

As Job Seekers

RESEARCH JOB DESCRIPTIONS

- Research job descriptions and look for patterns
- Pay attention to skills required
- Find companies that have similar values as yourself
- Beware of job descriptions that describe more of a whole team rather than a single role – burnout warning

EXPECTATIONS & INTEREST

- Level set your expectations – be realistic with salary expectations and current skillset – but don’t undersell yourself
- Determine which areas of cybersecurity interest you
- When breaking into the industry, be open to a variety of roles, they may give you new perspective
- Consider IT roles that intersect with cybersecurity when starting out

FIX SKILL GAPS

- Remember those patterns from the job descriptions? – Time to upskill!
- Home labbing – see the recording of my other talk
- Bootcamps/Certifications/Online Training (Check out BHIS/Antisyphon pay what you can courses)
- You get out what you put in

TAILOR YOUR RESUME

- Tailor your resume, not to a specific job, but rather a job function
- Highlight areas of experience – even if it is volunteer or home lab related (especially if you are starting out)
- Structure your resume to highlight what makes you the ideal candidate based on your experience (think above the fold)
- **Always be able to speak to anything you put on your resume**

NETWORK

- How many of you are hiring?
    - **Talk to these folks**
- Get involved in local professional groups like Bsides, ISSA, and InfraGard
- Make connections with likeminded folks on LinkedIn
- Get to know some recruiters – especially the corporate ones

SUMMARY

Hiring Managers

- Know Your Team & Needs
- Collaborate With Human Resources
- Improve Job Descriptions
- Improve Interview Process
- Network
- Be Realistic With Expectations

Job Seekers

- Research Job Descriptions
- Level Set Expectations & Determine Interest
- Fix Skill Gaps
- Tailor Resume to Job Function
- Network

Q&A

Thank you!

Michael Miller

mmiller.netsecdev@gmail.com

https://www.linkedin.com/in/michaelmillerdev/