

**JOB SEEKER  
OF**

**INFOSEC**

**POST COVID 19 EDITION**

# JOB SEEKER OF

# INFOSEC

POST COVID 19 EDITION



# DISCLAIMER



Opinions are my own and not the views of my employer

This talk is not sponsored by my employer or any organization

This talk is not a product, solution or service pitch

This material is not an ultimate guide, use with your own caution. **Not a guarantee for a new job**

# TABLE OF CONTENTS

## 01 – INTRODUCTION

- Disclaimers
- Contents for today
- Who am I

# TABLE OF CONTENTS

## 02 – THE JOBS

- Understanding the current job market
- Understanding the skills needed for common positions
- **Hands on – LinkedIn**
- Break

# TABLE OF CONTENTS

## 03 – HIRING SYSTEMS

- Understanding the hiring systems
- Understanding the stages of hiring
- **Hands on – Resume Writing with Canva**
- Break

# TABLE OF CONTENTS

## 04 – THE BALANCE

- What to do after all the process
- Keeping Physical and Mental Health in check

# TABLE OF CONTENTS

## 05 – CLOSING

- Resources
- Q&A



# 01

# INTRODUCTION

Disclaimers  
Contents for today  
Who am I

A black and white photograph of a person standing in a dark landscape at night, holding a large, glowing, translucent map or document. The background is a starry night sky with the Milky Way visible. The person is silhouetted against the bright light of the map. The entire image is framed by a thin white border.

# TAS

**@TAS\_KMANAGER** 

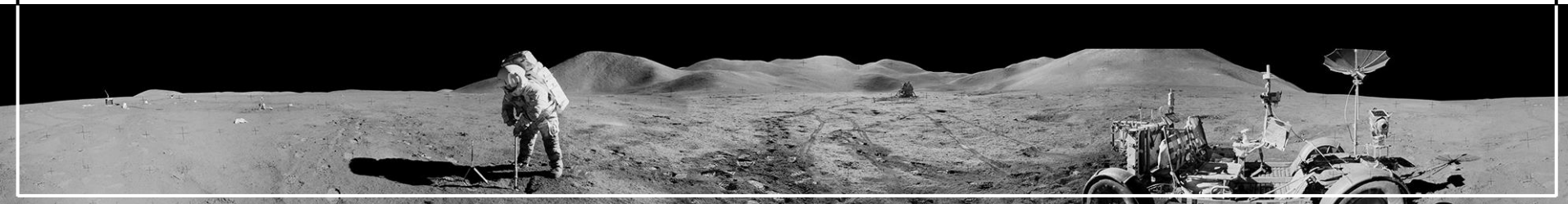
**/IN/TONDANGMANGATAS** 

Security Researcher @Major Tech Co.  
~5 Years Professional Career in Infosec

Contributor @TheDFIRReport

**HOW HARD CAN IT BE**

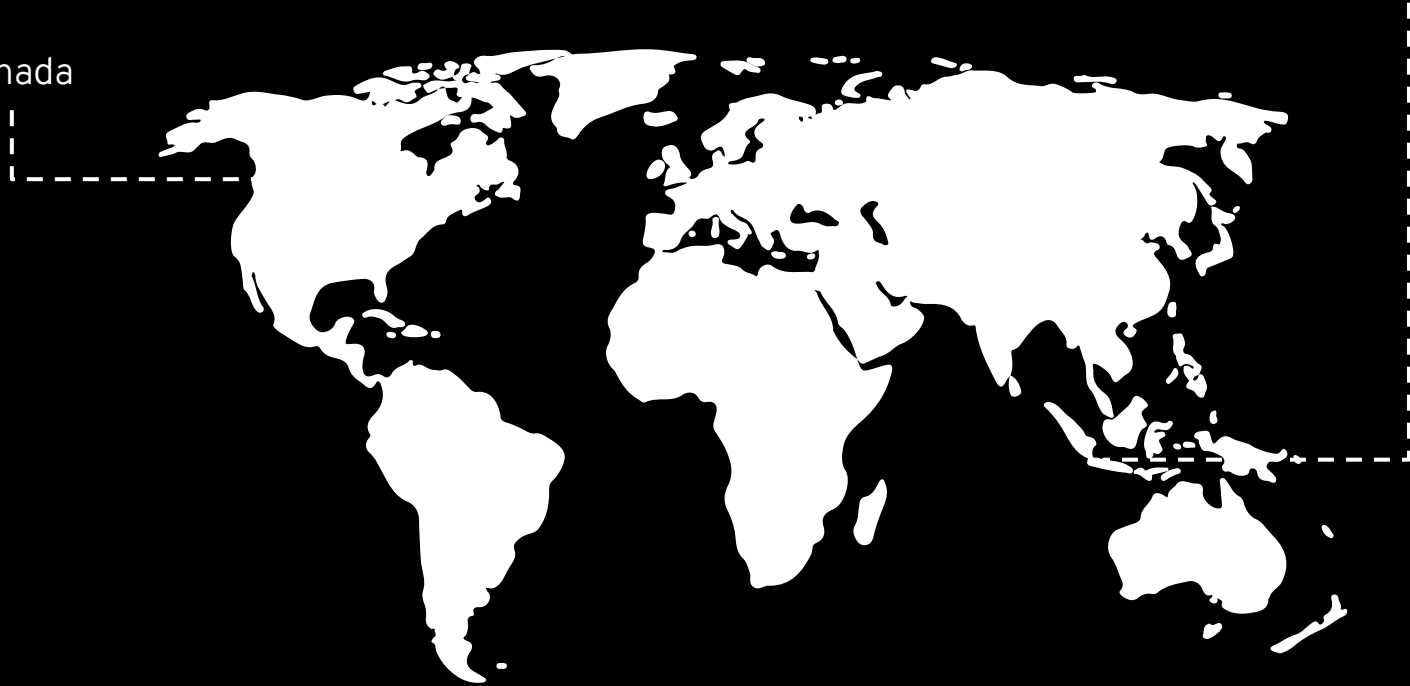
**TO FIND THE FIRST INFOSEC JOB ?**

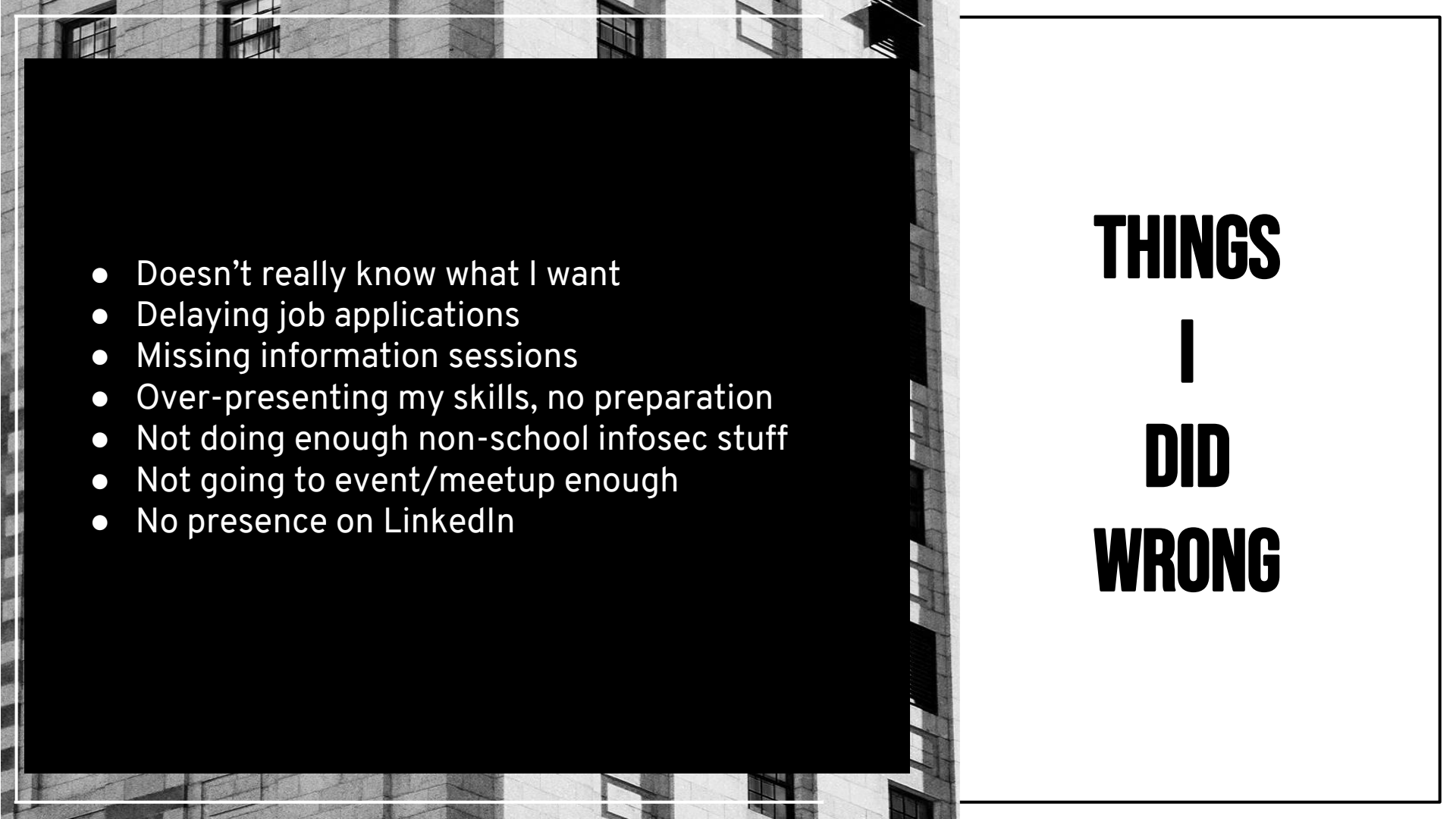


**FOR ME? IT WAS PRETTY HARD ☹️**

Canada

Indonesia



- 
- Doesn't really know what I want
  - Delaying job applications
  - Missing information sessions
  - Over-presenting my skills, no preparation
  - Not doing enough non-school infosec stuff
  - Not going to event/meetup enough
  - No presence on LinkedIn

**THINGS  
I  
DID  
WRONG**

# CAREER



**2017**

All Around Security

Health Tech Co.  
\*co-op/internship



**2017**

Application Security

Major Insurance Co.  
\*co-op/internship



**2018**

Threat Hunting

Major Telco Co.



**2020**

**Managed Detection & Response**

Big 4 Consulting Co.



**2022**

**Security Research**

Major Tech Co.

**CAREER**

# 02

## THE JOB

Understanding the current job market  
Understanding the skills needed for common positions  
**Hands on - LinkedIn**



# YOUR INFOSEC JOB EQUALS TO...



## LOCATION

Office vs Remote vs Hybrid  
Travel Requirement



## COMPANY

Type of Infosec companies  
Money? Benefit? Others?



## ROLE

Type of Position  
Job Description

# UNDERSTANDING THE CURRENT JOB MARKET

**Bloomberg**

Sign InSubscribe

• Live Now

MarketsTechnologyPoliticsWealthPursuitsOpinionBusinessweekEqualityGreenCityLabCryptoMore

Technology  
Cybersecurity

## Hackers' Path Eased as 600,000 U.S. Cybersecurity Jobs Sit Empty

- Job openings rose at double prepandemic rate in last 12 months
- Cyber professional shortfall could rise to 3.5 million by 2025

## FORTUNE | EDUCATION

ARTICLES RANKINGS MORE

In the U.S., there are about 1 million cybersecurity workers, but there were around 715,000 jobs yet to be filled as of November 2021, according to a report by [Emsi Burning Glass](#) (now [Lightcast](#)), a market research company. If so many bodies are needed to fill seats in cybersecurity roles, then what's the holdup on companies and universities preparing future professionals to take these jobs?



### U.S. BUREAU OF LABOR STATISTICS

#### [Job Outlook](#)

Employment of information security analysts is projected to grow 33 percent from 2020 to 2030, much faster than the average for all occupations.

About 16,300 openings for information security analysts are projected each year, on average, over the decade. Many of those openings are expected to result from the need to replace workers who transfer to different occupations or exit the labor force, such as to retire.

## **UNDERSTANDING THE LOCAL NEEDS**

Know where you can work, where can you relocate

- City or Metro Area
- Time zone
- National

Perform quick job search on each area online (LinkedIn, Indeed, etc.)

- Take notes on which opens role are out there
- What are the roles
- Which companies are hiring
- Which level (entry level, internship)
- How long the job has been posted

Check the news on these companies

- Layoffs
- Hiring Freeze
- Organization Activity (Acquisition, Merger, Funding, IPO, etc.)

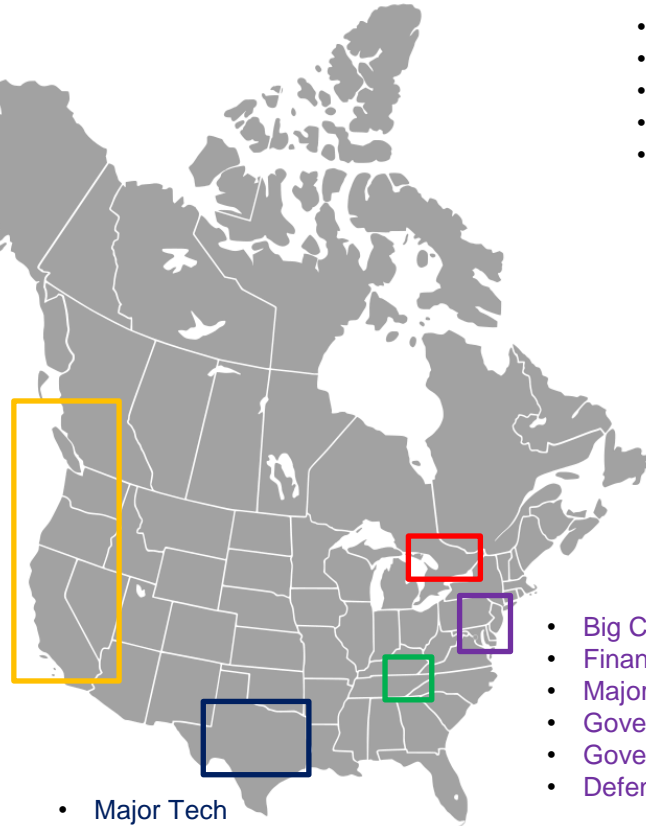
# LOCATION!!

All Over the Country

- Banks and Finance
- Regional and Local Government
- Small and Medium Business
- Consulting (MSP and MSSP)
- Educational
- Information Tech and Communication

(San Francisco, Seattle, Vancouver)

- Major Tech Hub
- Startups
- Security Vendors



- Canadian Big Corporation (Toronto)
- Canadian Major Tech Hub (Toronto)
- Finance (Toronto)
- Government/Contractor (Ottawa)
- Startups (Montreal, Waterloo)

- Big Corporation (NYC)
- Finance (NYC)
- Major Tech (NYC)
- Government (DMV)
- Government Contractor (DMV)
- Defense (DMV)

- Major Tech
- Energy

- Major Tech (ATL)

# **UNDERSTANDING THE REGIONAL/REMOTE NEEDS**

Majority of remote works out there still have constraints

- Need to be within office range for occasional visit
- Time zone
- Country specific

Some companies will have hiring “hubs”, even for remote roles

Americas:

- Canada
- USA

EMEA:

- Central and Western Europe
- UAE

APAC:

- Australia
- Singapore
- India



### Security Researcher - Mobile Malware (Remote)

CrowdStrike

Montreal, QC (Remote)

4 connections work here

Promoted



### Security Researcher - Mobile Malware (Remote)

CrowdStrike

Toronto, ON (Remote)

4 connections work here

2 days ago



### Security Researcher - Mobile Malware (Remote)

CrowdStrike

Finland (Remote)

4 connections work here

2 weeks ago



### Security Researcher - Mobile Malware (Remote)

CrowdStrike

Zurich, Zurich, Switzerland (Remote)

4 connections work here

2 weeks ago



### Security Researcher - Mobile Malware (Remote)

CrowdStrike

Copenhagen, Capital Region, Denmark (Remote)

4 connections work here

2 weeks ago



### Security Researcher - Mobile Malware (Remote)

CrowdStrike

Dublin, County Dublin, Ireland (Remote)

company alumni work here

2 weeks ago



### Security Researcher - Mobile Malware (Remote)

CrowdStrike

Reading, England, United Kingdom (Remote)

4 connections work here

2 weeks ago



### Security Researcher - Mobile Malware (Remote)

CrowdStrike

Sunnyvale, CA (Remote)

Medical benefit

 Actively recruiting

2 days ago

# EXAMPLE

# BUT DON'T LIMIT YOUR SEARCH BY THE LOCATION!

Although there might be location constraints, don't limit location while searching for a job

Why?

- Roles can be moved around if the company does business in the region
- Future roles might be opened in your area
- Roles can be converted in-to remote work
- A good way to create relation with recruiters and hiring managers
- Company might help with relocation

I DIDN'T KNOW THAT  
**COMPANY**  
IS DOING INFOSEC





## General Consulting

- EY
- Deloitte
- PwC
- KPMG
- Accenture
- MNP
- Avanade
- CGI
- Grant Thornton
- Thomson Reuters
- CDW
- Synopsys
- Thales
- BDO
- Capgemini

## Security Vendor & Consulting

- Mandiant
- Crowdstrike
- Blackberry (Cylance)
- Cisco (Talos)
- Intel 471
- Dell (SecureWorks)
- Palo Alto (Unit 42)
- Google TAG
- Microsoft MSTIC
- Cyderes
- Trellix
- Elastic
- OpenText
- Trend Micro
- Rapid7
- Cybereason
- Sophos
- Fortinet
- SentinelOne
- TrustedSec
- Black Hills Infosec
- FalconForce
- SpecterOps
- Red Canary
- Dragos
- Proofpoint
- IBM X-Force
- Recorded Future
- CloudFlare
- Kaspersky
- Huntress
- Okta
- NCC Group
- Jamf
- Objective-See

# CONSULTING COMPANIES

## Corporation

- General Electrics
- Boeing
- Raytheon
- Honeywell
- Samsung
- Siemens
- Bosch
- Santander
- TD
- Bank of America
- Wells Fargo
- JP Morgan
- Visa
- T-Mobile
- AT&T

- United Airlines
- Federal
- Chevron
- Walmart
- Target

## Government Contractor

- Federal LE
- Federal Departments
- Municipal Bodies
- MITRE
- Defense Contractors

## Tech Vendor

- Google
- Microsoft
- Amazon
- AWS
- Facebook/Meta
- Dropbox
- Cisco
- Apple
- IBM
- Dell
- Blackberry
- Netflix
- Spotify
- EA
- Sony
- Twitter

# IN HOUSE & TECH VENDOR COMPANIES

**BUT WHY WOULD I CHOOSE THEM?**

### **Financial**

Money/Mula/Bag/Cash/\$\$\$  
Stock options  
401K/RRSP contribution  
Bonus (complicated or not ?)  
JOB SAFETY

### **Benefit**

Health  
Fitness or Mental Health  
Family/Dependents

### **Flexibility**

Work from Home? Anywhere?  
Work at anytime  
Hands-off Management

### **People & Culture**

Industry  
Vision and Goals  
Community contribution  
Infosec “Public Figure”  
Tight knit group  
Working arrangement  
Team activities

### **Growth**

Training allowance  
Time off for training  
Conference/CTF  
Non-Infosec training  
Mentorship  
Can I learn from my work?

**REASONS  
TO  
PICK  
A  
COMPANY**

# LAMP METHOD

## **LIST**

Create a LIST of potential targets, 40+ is suggested

## **ALUMNI**

Create ALUMNI contacts

LinkedIn can be utilized for this purpose

## **MOTIVATION**

Score each target on scale 1 – 5  
with 5 denoting your dream employer

## **POSTING**

Do they have a job POSTING recently?

## **SORT, RANK AND MAKE CONTACT!**

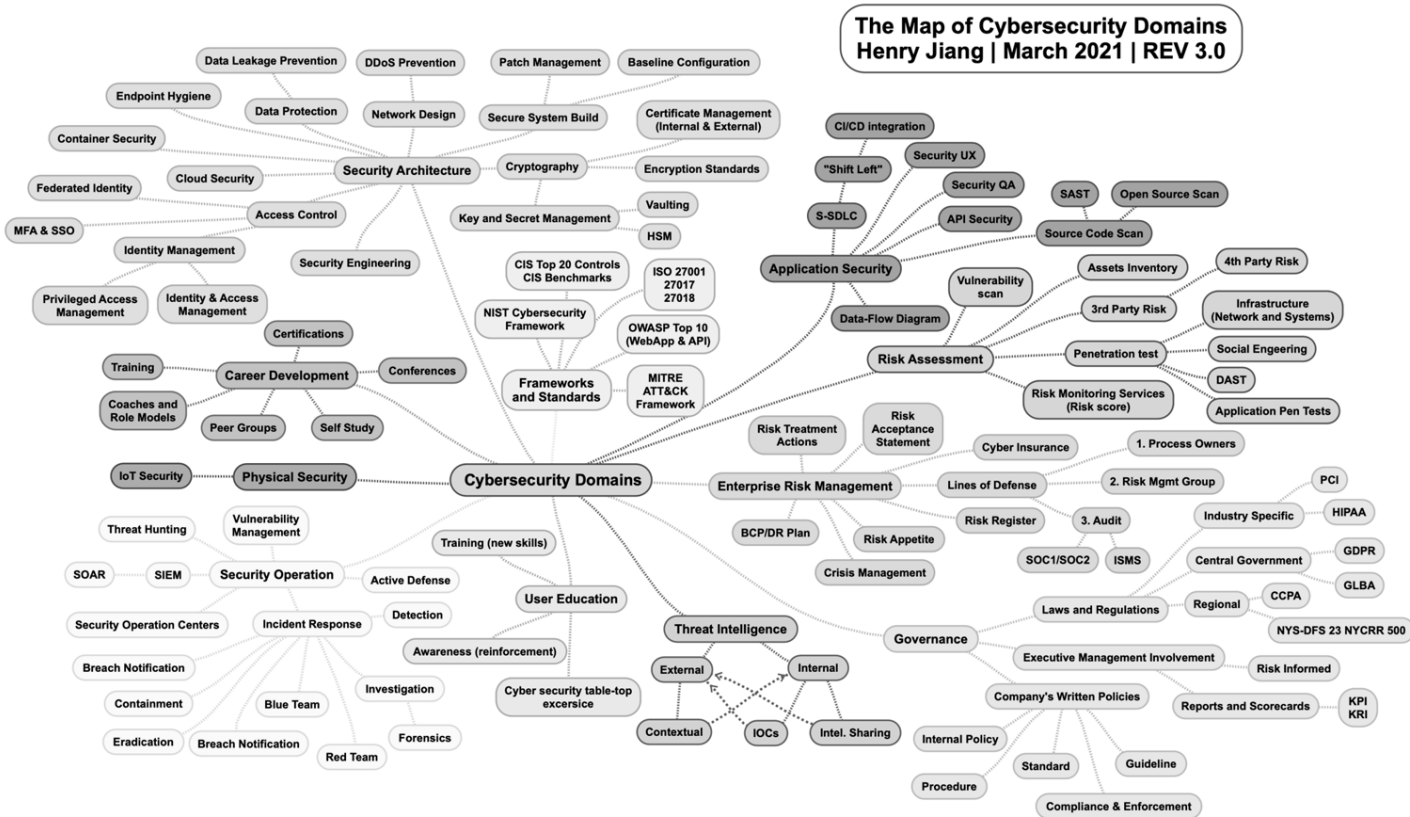
**SORT BY MOTIVATION, POSTING THEN ALUMNI**

# TO DO

## **Learn About The Company**

- Learn about the company, follow them in the news
- Was there any recent Layoffs or Hiring Freeze?
- Was there any recent Investment, Mergers or Buy Out?
- Understand the culture of the company
- Know why you “like” this company
- Talk to people in these companies e.g., via LinkedIn, Chat Group, or Meetup to understand more about the role
- Follow and Interact with their recruiter to get more insider insights

# I DIDN'T KNOW THERE ARE LOTS OF INFOSEC ROLES



## Offensive Operation

- Red Team Operator
- Penetration Tester
- Physical Penetration Tester
- Mobile Penetration Tester
- Offensive Security Engineer
- Offensive Security Specialist
- Ethical Hacker
- Bug Bounty Hunter (often called Security Researcher)

## Vulnerability Management

- Vulnerability Management
- Vulnerability Assessment
- Vulnerability Engineer

## Purple Team

- Adversarial Simulation
- Purple Team Engineer
- ATT&CK Assessment

## Research & Development

- Security Researcher
- Vulnerability Researcher
- Exploit Researcher
- Exploit Development
- Offensive Security Researcher
- Offensive Security Engineer
- Security R&D Engineer

# COMMON OFFENSIVE INFOSEC POSITIONS



# OFFENSIVE

## SKILLSET

- Attack Kill Chain
- OSINT
- Windows, Mac, and Unix internals
- Offensive security tooling  
(Bloodhound, NMAP, Meterpreter, C2 framework, etc.)
- CTF experience
- Exploit Development
- Programming
- Scripting
- Networking
- Social Engineering
- Reporting


# OFFENSIVE

## RESOURCE

- Awesome Red Teaming Tools [GitHub](#)
- Awesome Vulnerability Research [GitHub](#)
- Payload All The Things [GitHub](#)  
A list of useful payloads and bypasses for Web Application Security. Feel free to improve with your payloads and techniques
- SpecterOps [Blogs](#)
- MITRE Security Framework
  - [MITRE ATT&CK](#)
  - [MITRE ATT&CK Defender \(MAD\)](#)
- AD Attack Defense [GitHub](#)
- Awesome Cloud Security [GitHub](#)

Red Team Wireless Security Researcher

Apple · San Diego, CA

Apply 

Save

...

Key Responsibilities:

- \* Vulnerability research of wireless technologies covering radio firmware up through network stacks running on Apple devices
- \* Evaluate and design innovative exploit mitigations against evolving attacker techniques.
- \* Research and develop over-the-air attacks and defenses, including prototyping exploits to further inspire new defensive capabilities.
- \* Review software and hardware designs around wireless technologies and protocols.

Key Qualifications

Experience in (or strong drive to learn and define) the state-of-the-art wireless attacks in WiFi, cellular, NFC, or Bluetooth.

Ability to find, exploit, or mitigate attacks against wireless targets and respective software architectures (C/C++/ObjC/Swift).

Highly motivated and self-driven person with deep interest in understanding and exploring end-to-end wireless attacks.


A hands-on approach, and strong drive towards verifying and understanding wireless security postures and protocols.

Attention to detail and out-of-the-box thinking around security problems in a domain without excessive public knowledge around attacks.

# SAMPLE JOB POSTING

RED TEAM SECURITY RESEARCHER

Associate Penetration Tester - Red Team (Rem...  
Mandiant · Alexandria, VA (Remote)

Apply  Save ...

Responsibilities:

- Perform network penetration, web and mobile application testing, source code reviews, threat analysis, wireless network assessments, and social-engineering assessments
- Develop comprehensive and accurate reports and presentations for both technical and executive audiences
- Effectively communicate findings and strategy to client stakeholders including technical staff, executive leadership, and legal counsel
- Recognize and safely utilize attacker tools, tactics, and procedures
- Develop scripts, tools, or methodologies to enhance Mandiant's red teaming processes
- Assist with scoping prospective engagements, leading engagements from kickoff through remediation, and mentoring less experienced staff

Qualifications

Requirements:

- 2-5 years' experience in at least three of the following:
  - Network penetration testing and manipulation of network infrastructure
  - Mobile and/or web application assessments
  - Email, phone, or physical social-engineering assessments
  - Shell scripting or automation of simple tasks using Perl, Python, or Ruby
  - Developing, extending, or modifying exploits, shellcode or exploit tools
  - Developing applications in C#, ASP, .NET, ObjectiveC, Go, or Java (J2EE)
  - Reverse engineering malware, data obfuscators, or ciphers
  - Source code review for control flow and security flaws
- Strong knowledge of tools used for wireless, web application, and network security testing
- Thorough understanding of network protocols, data on the wire, and covert channels
- Mastery of Unix/Linux/Mac/Windows operating systems, including bash and Powershell
- Must be eligible to work in the US without sponsorship

# SAMPLE JOB POSTING

## PENETRATION TESTER

## Monitoring

- Security Analyst
- Threat Analyst
- Triage Analyst
- Security Specialist
- SOC Analyst
- MDR Analyst

## Intelligence

- Threat Intel Analyst
- Cyber Threat Intelligence (CTI) Analyst
- Security Researcher

## Detection & Response

- Threat Hunter
- Detection Engineer
- Detection & Response Engineer
- Threat Research Engineer
- Security Researcher
- Content Development
- Security Engineer
- SIEM Architect
- SIEM Engineer
- SOAR Engineer
- Security Data Engineer
- Solution Integrator
- Signature Developer
- Signature Engineer

- Security ML Engineer
- Security Data Scientist

## DFIR

- DFIR Consultant
- Forensic Analyst
- Incident Responder
- Incident Response Lead
- Incident Commander
- CIRT/CSIRT Analyst
- Malware Analyst
- Reverse Engineer

# COMMON DEFENSIVE INFOSEC POSITIONS

# DEFENSIVE/DFIR

## SKILLSET

- Critical Thinking
- Intrusion Analysis
- Log Analysis
- Forensic
- Windows, Mac, and Unix internals
- Cloud
- Networking
- SIEM familiarity
- AV/EDR operation
- Programming
- Scripting
- Reporting
- Communication
- Threat Mgmt.
- Sysadmin
- CLI
- Signature Building (YARA, Snort, etc.)

# DEFENSIVE/DFIR

## RESOURCE

- Awesome IR [GitHub](#)
- Awesome Threat Detection [GitHub](#)
- MITRE Security Framework
  - [MITRE ATT&CK](#)
  - [MITRE ATT&CK Defender \(MAD\)](#)
  - [MITRE D3FEND](#)
- [AwesomeDFIR.com](#)  
The definitive guide through the best articles, books, podcasts, tweets, tools, videos and newsletters to become a fantastic incident handler
- Prof. Messer Sec+ Free Course [YouTube](#)
- Awesome Cloud Security [GitHub](#)

## SOC Analyst II

DigitalOcean · NAMER (Remote)

Apply 

Save

...

### What You'll Add To DigitalOcean

- A high degree of curiosity and aptitude, with a clear passion around security as a lifestyle.
- Significant experience in one or more of the following fields:
  - Trust and Safety
  - Security Monitoring
  - Proactive Threat Hunting
  - Threat Intelligence Collection / Threat Investigation / Dissemination
  - Network Security / Cloud Security
  - Security Operations
- Ability to Diagnose, Troubleshoot, and Resolve Infrastructure Security Problems.
- Understanding of hardware, software, and networking; distributed computing; virtualization; high-performance storage systems; databases; and cloud computing.
- Understanding of fundamental TCP/IP concepts, application protocols and knowledge of database structures and working with Unix/Linux.
- Intellectual Curiosity and Self-Motivation to perform complex tasks.
- Clear written and verbal communication skills to include: technical writing, presenting, coaching, and mentoring.
- Ability to provide and receive clear, direct, and honest feedback for continuous improvement.
- The ability to remain optimistic and passionate about overcoming security obstacles at scale in both reactive and proactive situations.
- Consistently improving security as the platform scales, driving continuous improvement through data collection and correlation, being mindful that security should be an efficiency enabler for the business - not a detractor.
- Significant experience handling Incident Response in relation to live intrusions.
- A forward looking perspective on security engineering, tackling each problem with a degree of creativity that uses previous internal/external approaches as a data point, not a rulebook.
- Bonus:
  - Ability to code, script, or automate classes of problems rather than handling them manually (Python, Bash, Go, Ruby)

# SAMPLE JOB POSTING

## SOC ANALYST

## Cybersecurity Threat Intelligence Analyst

Chevron · Washington, DC

Apply 

Save

...

### As a Cybersecurity Threat Intelligence Analyst, You Will

- Leverage the threat intelligence lifecycle and priority intelligence requirements to track threat actors, research cyber threats, conduct analysis and create threat intelligence reporting to support Cyber Intelligence Centre's internal customers.
- Produce a variety of intelligence reporting from technical audiences to the executive level.
- Analyze external technical and non-technical data from various intelligence sources (paid, open and closed) to build threat actor profiles and track threat actor activities both externally and internally.
- Research new and emerging vulnerabilities, threat actor's tactics, techniques, and procedures, and conduct threat hunting within Chevron's environment for the presence of related activity.
- Collaborate with members of the Threat Intelligence team on emerging threats, cyber threat actor's activities, targeting and operational tempo.
- Prepare and deliver intelligence briefs to a variety of audiences.

### Experience

#### Requirements

- Past working experience working on a cyber threat intelligence team with experience analyzing, tracking and reporting on nation state, cybercrime and non-state supported threat actors.
- Experience working with the threat intelligence lifecycle and utilizing priority intelligence requirements to drive Chevron's intelligence operational workflow.
- Experience in leveraging analytic judgement to create high quality intelligence reporting.

### Skills

- Technical experience analyzing threat actor's tactics, technical and procedures: malware analysis, network traffic, endpoint activity and vulnerabilities and exploits.
- Leveraging analytic judgement to write high quality intelligence reporting with attention to detail and content that is relevant, accurate and timely.
- Technical analysis skills to analyze internal data and external information to hunt various threats.

### Education

- Bachelor's degree in related fields (Preferred)

# SAMPLE JOB POSTING

## CTI ANALYST

## Application Security & DevSecOps

- DevSecOps Consultant
- DevSecOps Engineer
- Security DevOps Engineer
- CI/CD Engineer
- Security Integration Engineer
- Solution Security Architect
- Product Security Architect
- API Security Engineer
- App Sec Engineer
- App Sec Consultant
- Software Security Engineer
- Product Security Engineer
- Secure SDLC Manager
- Software Engineer
- SAST/DAST Specialist
- Security Engineer

**COMMON  
APPSEC &  
DEVSECOPS  
INFOSEC  
POSITIONS**



## Infrastructure

- Infrastructure Security Engineer
- Platform Security Engineer
- Container Security Specialist
- Security Architect
- Cloud Security Architect
- Network Security Engineer
- Staff Security Engineer
- Security Data Engineer
- Security Systems Engineer

## Appliance / Technology Engineer

- IAM Specialist
- DDOS / WAF Engineer
- Firewall Engineer
- SAP Security Specialist
- Endpoint Security Engineer
- Security ML Engineer
- UEBA Engineer
- X Integration Engineer
- X Integration Consultant
- OT Security
- IoT Security

# COMMON INFRA & ENGINEER INFOSEC POSITIONS

## APPSEC/DEVSECOPS/INFRA/ENGINEER

### SKILLSET


- Programming
- Instrumentation  
(Chef, Puppet,  
Ansible, etc.)
- Container, Docker,  
Kubernetes
- Database or Big  
Data
- Cloud  
environments
- OWASP
- Secure Coding
- QA Test
- SAST/DAST
- SDLC
- CI/CD
- Vendor Specific  
Tool

## APPSEC/DEVSECOPS/INFRA/ENGINEER

### RESOURCE

- Awesome AppSec [GitHub](#)
- Awesome DevSecOps [GitHub](#)
- DevSecOps roadmap [GitHub](#)  
Roadmap for everyone who wants DevSecOps.

Application Security Consultant (Remote, Unit...  
Synopsys Inc · United States (Remote)

Apply 

Save

...

Responsibilities

- Lead security engagements
- Perform application security assessments such as web application, mobile, API, or thick client penetration tests
- Analyze application architecture for security design flaws
- Provide security guidance to organizations designing cloud applications
- Assist organizations with the automation of security activities through DevSecOps principles and best practices
- Other ad-hoc duties as required

Required Qualifications

- Ability to interface with clients, utilizing consulting and negotiating skills
- At least 1 year of work experience in Application Security, Cyber Security or similar
- Some experience performing security assessments on applications
- Understanding of common web application security issues i.e., OWASP Top 10 and SANS Top 25
- Bachelor's degree in Computer Science/Engineering or equivalent experience
- Must be eligible to work in the United States without requiring sponsorship now or in the future
- Must be able to travel up to 25% of the time as required (estimated)

Nice To Have Qualifications (Not Required)


- Familiarity with software security weakness, vulnerability and secure code review a plus
- Familiarity with software attack and exploitation techniques a plus
- Familiarity with at least one software programming language and framework a plus
- AWS or Microsoft Cyber Security Certifications

# SAMPLE JOB POSTING

## APPSEC

### Infrastructure Security Engineer

Palantir Technologies · Denver, CO

Apply 

Save

...

#### Core Responsibilities

- Design, architect, and implement defensive security controls across endpoints (MacOS, Windows), servers (Linux), and SAAS/self-hosted applications.
- Provide security domain expertise on protective controls, to include system, network, encryption, and authentication services.
- Design, architect, and implement defensive security controls for e-mail (SPF, DKIM, DMARC, attachment sandboxing, etc.) and other collaboration applications.
- Collaborate with engineering teams to improve security for identity access and management (IAM), device management, and public cloud service providers (e.g. Amazon AWS, Google GCP, Microsoft Azure).
- Perform security evaluations and research on new platforms, products, architectures, vendors, and services to protect Palantir data.
- Partner closely with other members of the Technical Operations, Engineering, and Information Security teams to drive impactful changes to the company's network defense posture.

#### What We Value

- 3+ years of direct information security experience with deep exposure in protecting one or more operating system platforms (Windows, MacOS, or Linux).
- Comprehensive knowledge of modern adversary tactics, techniques, and procedures.
- Ability to independently own projects and balance competing priorities, whilst still effectively collaborating with colleagues.
- Experience with public cloud service providers (e.g. Amazon AWS, Google GCP, Microsoft Azure).
- Experience with infrastructure automation platforms (e.g. Desired State Configuration, Packer, Terraform, etc.).
- Proficiency with at least one scripting language (e.g. PowerShell, Bash, Python, or similar).
- Willingness and eligibility to obtain a U.S. security clearance, or active TS//SCI.

# SAMPLE JOB POSTING

## INFRA SECURITY ENGINEER

## Governance, Risk & Compliance

- GRC Specialist
- GRC Consultant
- Risk Management
- Security Audit
- Security Officer
- Compliance and Audit Manager
- Technology Risk Consultant
- Information Risk Specialist
- IT Risk Specialist
- Security Policy and Standard
- Privacy Officer
- Strategic Consulting
- Security Strategy

## Program / Project Manager

- Technical Program Manager
- Program Manager
- Delivery Manager
- Project Manager
- Product Manager – Security
- Account Manager
- Security Product Owner
- Security Transformation Manager
- Security Services Program Manager
- Agile Specialist
- Scrum Master

# COMMON GRC & PM INFOSEC POSITIONS

# GRC & PM

## SKILLSET

- GRC Platforms
- IT Risk Mgmt.
- Audit
- Policy Mgmt.
- Risk Assessment
- Metric
- Data Analytics
- Industry Standards (CobIT, ISO, PCI DSS)
- Government Regulation (GDPR)
- Presentation
- Reporting
- Attention to Details
- Project Management
- Planning
- Communication

# GRC & PM

## RESOURCE

- Awesome GRC [GitHub](#)
- Common GRC Standards
  - Sarbanes-Oxley Act - [SOX](#)
  - General Data Protection Regulation - [GDPR](#)
  - Payment Card Industry Data Security Standard - [PCI-DSS](#)
  - Health Insurance Portability and Accountability Act - [HIPAA](#)
  - International Organisation for Standardization's Information Security Management Standard - [ISO 27001](#)
  - Systems and Organization Controls for Service Organizations: Trust Services Criteria - [SOC2](#)
  - Federal Risk and Authorization Management Program - [FedRAMP](#)
  - Federal Information Security Modernization Act - [FISMA](#)
- Awesome PM [GitHub](#)

### GRC/IRM Technology Solutions Consultant-Sr....

PwC · Birmingham, AL (Remote)

Apply ↗

Save

...

Demonstrates thorough abilities and/or a proven record of success in roles performing on GRC and IRM programs. These projects should be targeted to enable multiple business processes and/or source data systems to drive efficiencies and reduce redundancies supporting one or more of the following functions: internal audit, compliance, enterprise risk management, operational risk management, technology risk management, third party risk management, cyber security, business resiliency, incident management, SOX (and/or other compliance frameworks), or other business programs/initiatives. In specific, the following skills are aligned with this position:

- Risk management, compliance management, and/or enterprise governance as it relates to how technologies can be and are leveraged throughout organizations' internal audit, risk and compliance functions and processes, as well as the associated benefits that can be realized;
- Integrated risk management (IRM) frameworks, especially as it relates to building a program or capabilities across an enterprise;
- Experience in designing, reengineering, optimizing, and documenting financial, operational, technology, and business requirements, processes and workflow related to any of the listed GRC functions above through stakeholder interviews, facilitated workshops, and analysis of client process documentation;
- Experience in creating, drafting, and refining core business foundational elements such as process, risk, and control frameworks related to any/all of the listed GRC functions above through stakeholder interviews, knowledge of industry leading practices and frameworks, facilitated workshops, and analysis of client process documentation;
- Deep understanding of access control, specifically role based access and inheritance of role and record based permissions;

# SAMPLE JOB POSTING

## GRC

## Security Program Manager

Microsoft · Redmond, WA (Hybrid)

Apply ↗

Save



### Qualifications

- A minimum of 2 years of technical program management experience in Cybersecurity or software development field
- Bachelor's degree in Computer Science, Engineering, or a related technical field or equivalent experience

### Preferred

- Unwavering passion for our customers
- In-depth knowledge of security concepts
- Have strong interpersonal, oral, and written communication skills
- Knowledge of the Security Development Lifecycle (SDL)
- Professional case management, triage, or release experience
- Experience investigating security vulnerabilities and exploits
- Experience debugging code
- Experience in creating content for security or technology professionals
- Strong domain knowledge on security vulnerabilities and security incidents
- Ability to distill and explain complex technical and security concepts to different types of audiences
- Track record of executing programs across highly matrixed and cross functional environment
- Experience collaborating with the vulnerability research community is a plus

**SAMPLE  
JOB  
POSTING  
PM**



**THERE  
ARE  
MORE**

## Non-Standard Security Role

- Customer Success Specialist
- Security Support Engineer
- Account Manager
- Account Executive
- Territory Manager
- Recruiter
- Community Manager
- Security Sales
- Technical Writer
- Content Builder
- Technical Trainer
- Executives
- Legal
- Cyber Insurance Specialist

# TO DO

## **Learn About The Role**

- Know the positions you want, rank them as per LAMP
- Talk to people with these positions e.g., via LinkedIn, Chat Group, or Meetup to understand more about the role
- Go through job posting to familiarize with job description
- Understand the skillset required for each positions
- Match your skillset with your dream job (BY WORKING ON IT!)



**LEVEL  
UP**

## Offense

- Join offensive community (Bloodhound Gang, Red Team Village, etc.)
- Participate in local Conference and CTF (Bsides or OWASP)
- Do OverTheWire, TryHackMe, HackTheBox online CTF
- Build home lab and deploy offensive security tools (Caldera, C2 Framework, etc.)
- Read offensive security books (RTFM, Hacking art of exploitation, etc.)
- Build your own tool (C2, Recon tool, etc.)

## Defense

- Join defensive community (TrustedSec, BHIS, OTR, etc.)
- Participate in local Conference and CTF (Bsides or OWASP)
- Do CyberDefenders and BlueTeamLabs online CTF
- Build home lab and deploy defensive security tools (SIEM, Firewall, Sysmon)
- Read defensive security books (BTfM, Practical Malware Analysis, etc.)
- Getting familiar with the tools (Debugger, Decompiler, Memory Forensic tools)

**LEVEL  
UP  
CONT.**

# LEVEL UP CONT.

## AppSec

- Learn about Container technology
- Learn about Cloud technology
- Try Leet Code and code more (display it in Github)
- Understand and apply Git Hygiene
- Deploy infra tools in your home lab (Deploying set of servers with Ansible, etc.)
- Dig deeper on OWASP and CVE
- Join Infrastructure/AppSec community (Tools specific, OWASP chapters, etc.)
- Code even more 😊
- Familiarize with SDLC and Agility concept

Lesley Carhart's Blog:

<https://tisiphone.net/2015/11/08/starting-an-infosec-career-the-megamix-chapters-4-5/>

Sheridan College - John Simpson's

“The Wonderful World of Information Security 2021”:

<https://docs.google.com/presentation/d/1kD6TdAq6c2pB6PYxhiEH0IIVjj6ZZ-9M/edit#slide=id.p7>

**GREAT  
RESOURCES!**

# TO DO

## Build Your Profile

- Maximize your online professional profile *(NEXT WORKSHOP PART)*
- Share your journey (Blogging, GitHub, Presentation)
- Join Online Community such as Infosec Knowledge Sharing (BHIS) Discord or Bloodhound Gang Slack
- Join local in person conference such as BSides or OWASP
- Join Newcomer conference such as SANS New2Cyber, PancakesCon or BSides Proving Ground
- Watch SANS Presentation on YouTube
- Follow Cyber Security News such as ThreatPost or tl;dr sec newsletter
- Join Open-Source community (OSCD, Open Threat Research, SIGMA, etc.)



BREAK TIME



# HANDS ON LINKEDIN



# MAXIMIZING YOUR PROFILE

- **Complete all information section**
  - Including additional stuff such as volunteer experience, project, organization, featured and license/certs
- **Use professional photo**
  - It can be a fun one but definitely not I-wake-up-like-this selfie!
- **Create a tailored summary and headline**
  - This section should highlight your key competencies and your passions in a form of story
  - Often recruiter decide to visit your profile based on this
- **Share updates and interact with people posts**
  - As simple as sharing the latest cyber news or liking other practitioner post
  - Being genuine, get involved in the discussion not just replying with “nice post”
  - LinkedIn can be used as blogging platform when you are ready
- **Join LinkedIn Group according to your Cyber Security preference**
- **Create a personalized LinkedIn address**
- **Connect with your real-life connections first**
  - Your classmates, your current job coworkers, local conferences attendees
  - Some conference or group chat platform might have LinkedIn connection rooms

# SETTING UP LINKEDIN JOB SEARCH

<https://www.linkedin.com/jobs/search/>

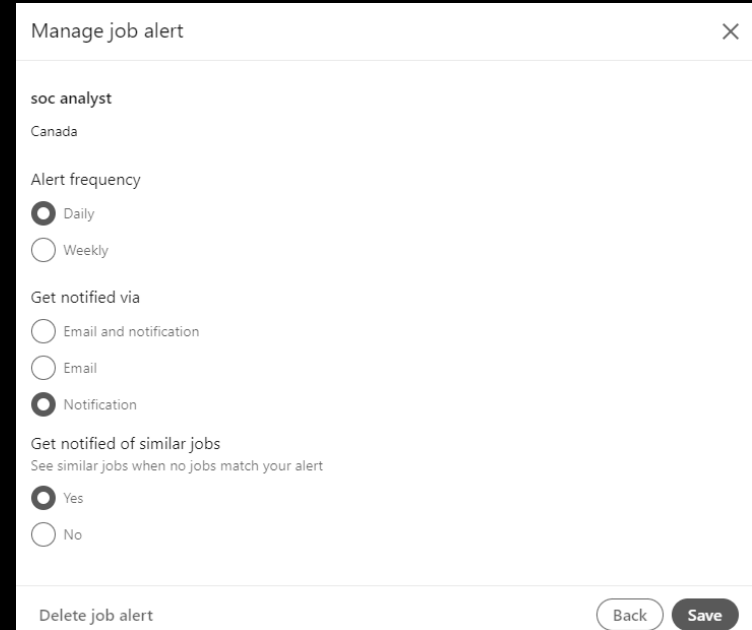
Two main components:

- LOCATION
- ROLE/TITLE/SKILL

Everything else is optional and sometimes they are prohibiting you from seeing more results

Setup the alert to be like the screencap

- Use daily if you are actively looking for jobs, weekly if not
- Always select Yes for similar jobs notifications, YES, THEY WORK WELL!



The screenshot shows the 'Manage job alert' dialog box on LinkedIn. It has a title bar with a close button (X). The main content area is white with a light gray border. The settings are as follows:

- Job Title:** soc analyst
- Location:** Canada
- Alert frequency:** ☒ Daily, ☐ Weekly
- Get notified via:** ☐ Email and notification, ☐ Email, ☒ Notification
- Get notified of similar jobs:** See similar jobs when no jobs match your alert. ☒ Yes, ☐ No

At the bottom, there is a 'Delete job alert' link on the left and 'Back' and 'Save' buttons on the right.

# WAYS TO DIVIDE THE SEARCH

- Location + Skills/Role

- Include specific location time zone or region in addition to the role
- E.g.
  - California + SOC Analyst
  - DC + SOC Analyst
  - Remote + SOC Analyst






- Company + Skills/Role

- Include the company you want in addition to the skills or role
- E.g.
  - Microsoft + MITRE ATT&CK
  - Microsoft + Penetration Test
  - Mandiant + Penetration Test

- Skills/Role


- Try to catch all the role that are there in the world
- This can help you to understand the current market and hiring location trends
- Might be hard to go through everything in 1 sitting

# MY OWN JOB SEARCH RESULT

	Your Job Alert for security engineer in Singapore	11h
	<a href="#">View 30+ Jobs</a>	...
	Your Job Alert for cyber security in Greater Vancouver, BC	12h
	<a href="#">View 30+ Jobs</a>	...
	Your Job Alert for threat hunting in Australia	12h
	<a href="#">View 1 Job</a>	...
	Your Job Alert for cyber security in Indonesia	13h
	<a href="#">View 7 Jobs</a>	...
	Your Job Alert for detection and response in Worldwide	14h
	<a href="#">View 30+ Jobs</a>	...

**INTERACT WITH THE RESULT**

# LET THE LINKEDIN ML/AI DO ITS JOB!




CrowdStrike is hiring: **Threat Analyst (Remote, AUS)**. See this and 3 other job recommendations.

7h


...

[View jobs](#)


### Jobs based on your Profile




**Threat Analyst (Remote, AUS)**  
CrowdStrike  
Sydney, New South Wales, Australia (Remote)  
131 company alumni work here  
2 weeks ago · 23 applicants




**Data Privacy Engineer-GoTo Financial**  
Gojek  
Jakarta, Jakarta, Indonesia  
2 connections work here  
20 hours ago




**Sr. Intelligence Analyst (Asia Pacific)**  
CrowdStrike  
New Brunswick, Canada (Remote)  
131 company alumni work here  
Promoted



**Senior Application Security Engineer**  
ConsensSys  
Canada (Remote)  
24 company alumni work here  
Promoted · 12 applicants



**Staff Product Security Engineer**  
Five9  
Canada (Remote)  
10 company alumni work here  
Promoted



**Senior Threat Intelligence Analyst (Remote Canada)**

## Threat Analyst (Remote, AUS)

CrowdStrike · Sydney, New South Wales, Australia (Remote) · 2 weeks ago · 23 applicants

**Full-time · Entry level**

1,001-5,000 employees · Computer and Network Security

4 connections · 131 company alumni · 2 school alumni

See recent hiring trends for Mozilla. [Try Premium for free](#)

You have a preferred skill badge

[Apply](#) [Save](#)

#WeAreCrowdStrike and our mission is to stop breaches. As a global leader in cybersecurity, our team changed the game. Since our inception, our market leading cloud-native platform has offered unparalleled protection against the most sophisticated cyberattacks. We're looking for people with limitless passion, a relentless focus on innovation and a fanatical commitment to the customer to join us in shaping the future of cybersecurity. Consistently recognized as a top workplace, CrowdStrike is committed to cultivating an inclusive, remote-first culture that offers people the autonomy and flexibility to balance the needs of work and life while taking their career to the next level. Interested in working for a company that sets the standard and leads with integrity? Join us on a mission that matters - one team, one fight.

### About The Role

The CrowdStrike EndPoint Protection (EPP) Content product group is seeking a motivated individual with technical skills to join our Threat Efficacy team. As part of the team, you will monitor and analyze the multitude of detections and preventions deployed by the various teams within CrowdStrike. The primary goal of this team is to respond to customer inquiries about threat detections and capabilities, proactively manage false positives, and increase the overall efficacy of our content.

This role will work closely with internal teams such as Technical Account Managers, Falcon

- 
- ~~Doesn't really know what I want~~
  - ~~Delaying job applications~~
  - ~~Missing information sessions~~
  - ~~Over-presenting my skills, no preparation~~
  - ~~Not doing enough non-school infosec stuff~~
  - ~~Not going to event/meetup enough~~
  - ~~No presence on LinkedIn~~

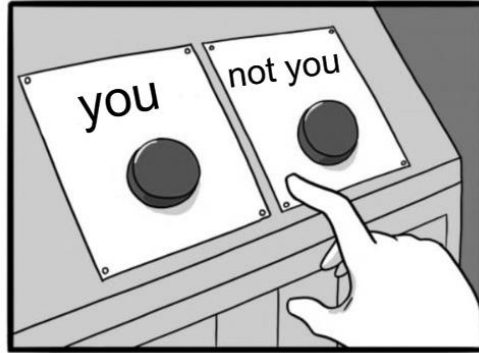
**THINGS  
I  
DID  
WRONG**



# 03

# HIRING SYSTEMS

Understanding the hiring systems  
Understanding the stages of hiring  
**Hands on – Resume Writing with Canva**



imgflip.com

JARE-CLARK.TUMBLR

# UNDERSTANDING THE HIRING SYSTEMS

# NAVIGATING AROUND ATS

ATS = Applicant Tracking Systems (automated ranking systems too)

How it works: [Jobscan.co](https://www.jobscan.co)

Tips and Tricks:

- **DON'T LIE ABOUT YOUR SKILLS!** Make sure that you are qualified
- Don't apply to all jobs for one company, pick one or two
- Mimic the job description keywords
- Have a skills section with both short and long version of the skills, such as SIEM and Security Information Event Management
- Tailor resume for certain group of jobs, for example one for SOC Analyst, one for Incident Responder, etc.

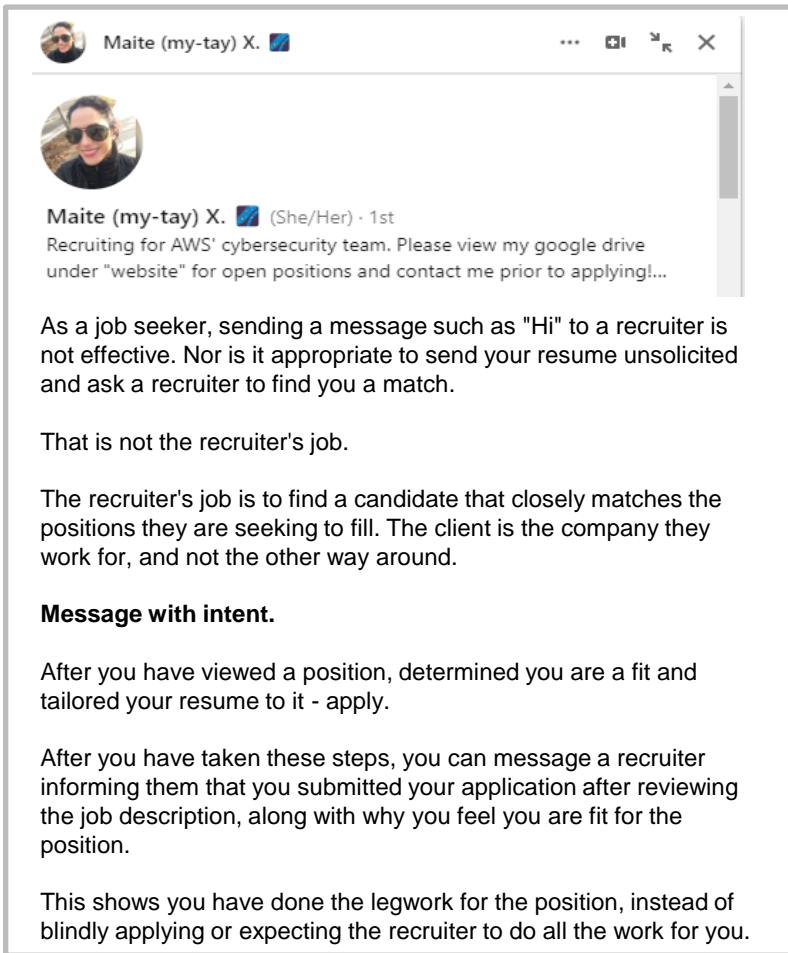
# RECRUITERS AND CONNECTIONS

## **Recruiters:**

A good recruiter is there to support you and advocate your demands

Tips on working with Recruiter:

- Find a good recruiter (based the way they approach you, the way they post a job, based on their answers to questions, etc.)
- It's a team effort, you must look for the role too (within their scope)
- Come prepared and set goals first (aka dream role)
- Ask the right questions (about the role, about timeline, about the company, etc.)
- Nothing is instant and keep track of the application. Follow up when needed, note that they are probably talking to other candidates too.
- Be nice, all the time!



# RECRUITER SAYS...

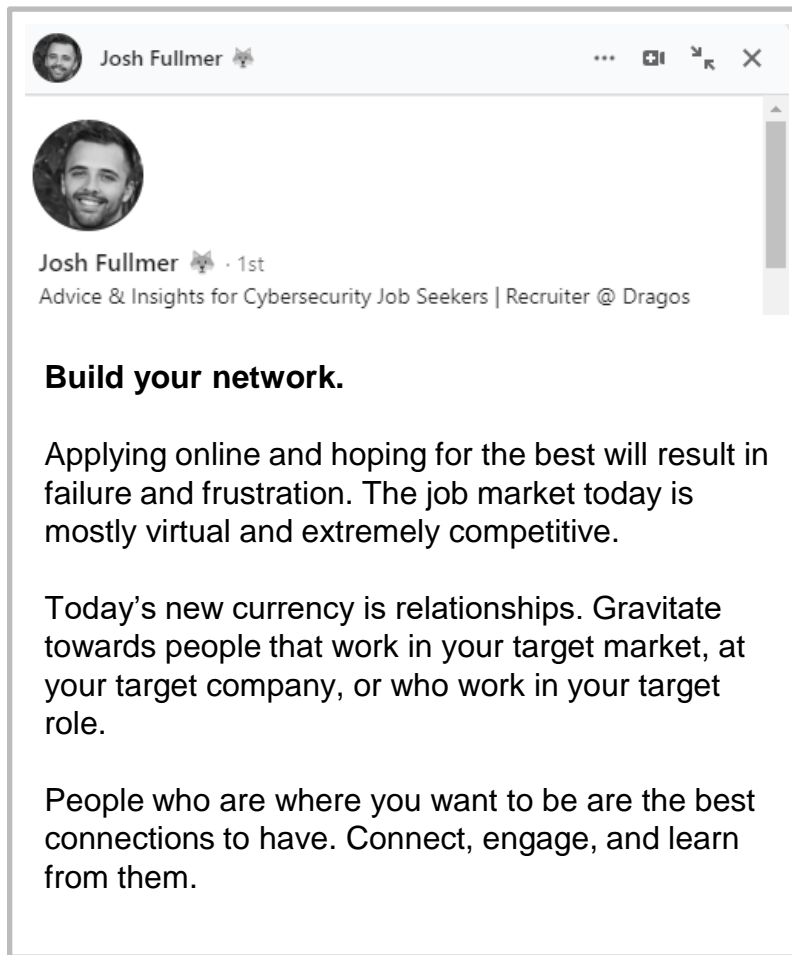
# RECRUITERS AND CONNECTIONS CONT.

## **Connections:**

A good connection can be used as a reference to a role or just simply to learn and discuss cyber security related topics.

Best places to find connections:

- Workplace! Start with your team and expands to other teams
- Local conferences or community such as BSides or OWASP chapters, take courage to initiate conversation during the break
- Regional or International conferences. Volunteer, attend their demo, workshops, training and talks and engage during the activity
- Open-Source Projects community such as contributing to SIGMA detection project
- Trainings, workshops or classes, interact with other students and attendees
- Genuine respond and comment during online discussion such as in LinkedIn or Chat Group (Discord, Signal, Slack, etc.)



**RECRUITER  
SAYS...**

**PROTECTING  
YOURSELF**





## **APT Lazarus LinkedIn Campaign**

The attacker pose as recruiter offering job from reputable company.

Attacker send malicious document

Malicious document ran by the user and attacker have full access to the user machine

Link: [ThreatPost](#)

## **Financial Scam**

Attacker pose as recruiter from major company.

Process continued all the way to hiring.

They asked to ship the most expensive phone to their “technician” address or asked for the applicants' details such as Social Security Number

# **REAL LIFE THREAT AGAINST JOB SEEKER**

# SPOTTING THE THREAT

## **Fake LinkedIn Users:**

- Verify their connections, work history, recent posts, etc.
- Ensure the profile picture is not AI generated / GAN
- Perform quick search on their description, some might just be a copy paste

## **Fake Recruiters:**

- Non corporation email address (such as Gmail or Yahoo)
- Everything seems so urgent (recruiter keep asking for update)
- No camera being used during online meetings or no in person meeting
- Using unusual mode of communication (such as WhatsApp)
- Lot of mistakes in the communication, letter, etc.

## **Financial Scam:**

- Asking for financial information to be sent using unsecured channel
- Asking to send expensive items or money
- Asking to pay for a fee, such as background check or others
- Way too high salary offer



# **UNDERSTANDING THE HIRING STAGES**

# PREPARATION

Know what you want and what you don't want!

Prepare the 3 components of a job; Role, company and location

- Role: several position you want or based on the types
- Company: your target companies that will fit you well
- Location: Where do you want to or can work

Understand the requirements for each roles

Utilize LAMP method explained previously

**Level up, making real connection and do your research!**

## Utilize Professional Social Media

Setup job alerts on these sites:

LinkedIn (Jobs)  
Glassdoor  
Indeed

Combine the search terms on  
the position section

Interact (respectfully) with the  
employees and recruiters

## Being Strategic

Keep an excel sheet to keep  
track of found application with  
these information

Position  
Company  
Closing Date  
Link to Job Posting  
Contact Point  
Reference Material  
Ranking  
Notes

# SEARCHING

## Entry Level Position

Look for role with these terms:

Junior / Jr.  
Entry Level  
Associate  
Graduate  
New Graduate  
Graduate Program  
Early  
L1 / Level 1  
T1 / Tier 1  
Triage  
Analyst

## Co-op Position

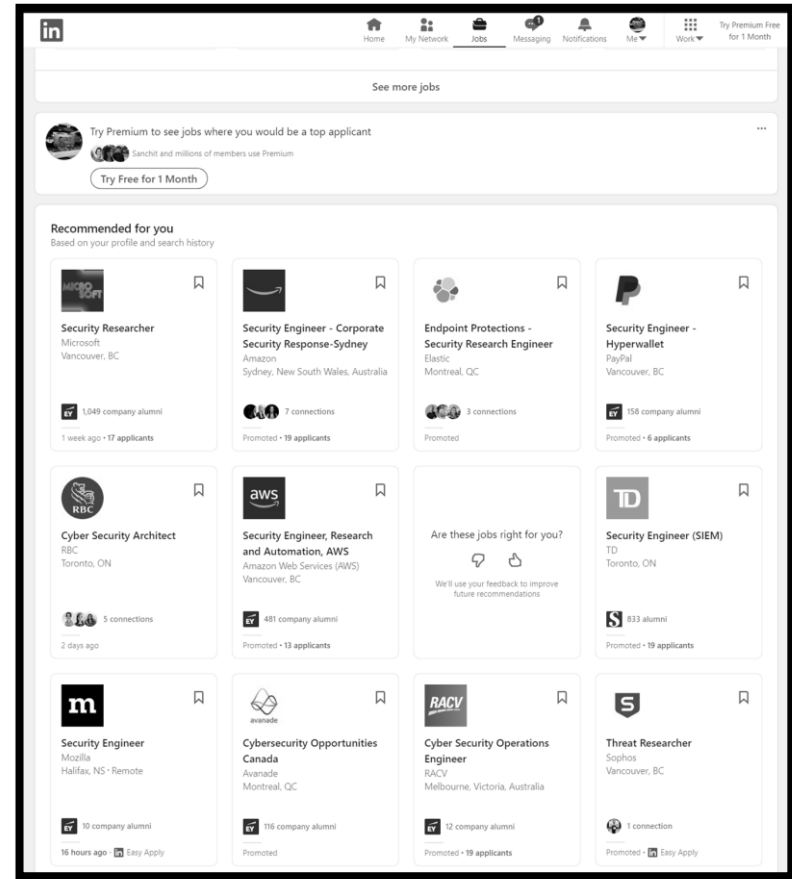
Look for role with these terms:

Co-op  
Intern  
Internship  
Trainee  
Apprentice (UK)  
Placement  
Working Student  
Winter/Summer/Fall 2022

# STARTING UP KEYWORDS

## Let the Algorithm do the job!

- Create multiple job alert
- Algorithm will learn over time
- Recommendation will start coming
- You can even “save” jobs you are interested in on LinkedIn



# RESUME

## CONTACT INFORMATION

### SUMMARY

### EDUCATION

### EXPERIENCE

### SKILLS

### ADDITIONAL INFO:

COMMUNITY INVOLVEMENT

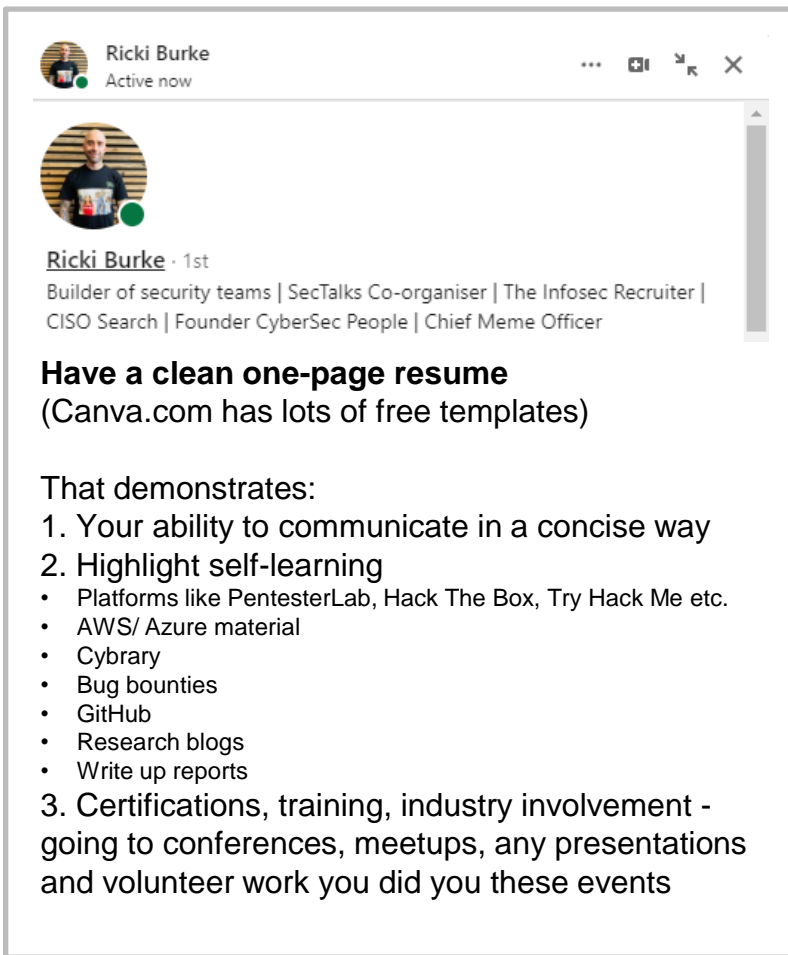
HOBBIES

VOLUNTEER EXPERIENCE

PUBLICATIONS

- Keep it short (2 pages max), concise and simple
- Tailored towards the position job description, try to add the keywords to pass the HR filter
- Add data to your story; 3x faster, 25% less cost, etc.
- Explain your experience thoroughly, sometimes small details can cause big impacts
- Focus on I (what you are doing) not we
- Write cover letter, when possible
- Include LinkedIn, GitHub or professional/research website
- Minimize white space, but still leave some for “sectioning”
- Use professional email and contact information
- Follow the file format requirement (e.g., if they accept PDF)
- Keep the “paste-able” information ready to use for filling application form (can be saved on .txt file)
- Ask for peer review from professor, career advisor or friend/family





**RECRUITER  
SAYS...**

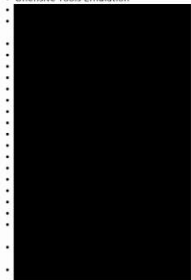
# MANGATAS TONDANG

THREAT HUNTING AND DETECTION ENGINEERING

Mississauga, Canada | +1 [REDACTED] [REDACTED]

## PROFESSIONAL SKILLS

- Threat Hunting Operation
- Threat Intelligence Operation
- Offensive Tools Emulation



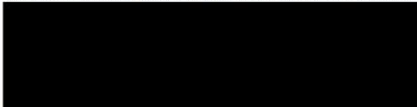
## TECHNOLOGY EXPERIENCE

- Scripting (Python, PowerShell, Bash, Batch, Jupyter Notebook)
- Programming (Java and C)
- Pattern Matching (Regex, YARA, Snort, Sigma, KQL/Lucene, SPL)



## SUMMARY

Mangatas is a CompTIA Security+ certified with 3+ years professional experience mainly in Threat Hunting, Threat Intelligence, and Incident Response powered by

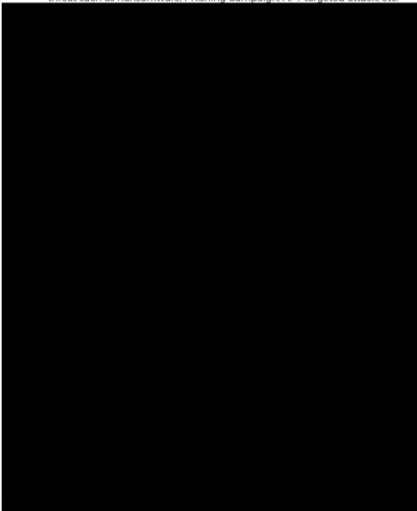


## WORK EXPERIENCE

### SENIOR CONSULTANT, MANAGED DETECTION AND RESPONSE (MDR)

Ernst & Young (EY) - Toronto, Canada | Nov 2020 - Now

- Lead Incident Response procedure in client environment (from planning all the way to the post-incident activity such as reflection and reporting) against threat such as Ransomware, Phishing Campaign, APT targeted attack, etc.



# MANGATAS TONDANG

THREAT HUNTING AND DETECTION ENGINEERING

Mississauga, Canada | [REDACTED] [REDACTED]

## COMMUNITY ACTIVITIES

- Sheridan College ISSessions
  - Member
  - Guest Speaker
  - CTF Challenge Developer
- HackFest Conf. (Quebec City)
  - Conf. Presenter - 2019



## CERTIFICATIONS AND COURSES

- CompTIA - Security+
- MITRE ATT&CK Defender Cert.
  - SOC Assessment



## CONTACT

Cell:



Email:



LinkedIn:

[linkedin.com/in/hondangmangatas/](https://www.linkedin.com/in/hondangmangatas/)

GitHub:

[github.com/hx-mangatas/](https://github.com/hx-mangatas/)

\*presentation slides can be found here

## EDUCATION

### BACHELOR OF APPLIED INFORMATION SCIENCES (BAISC)

#### INFORMATION SYSTEMS SECURITY

Sheridan College | Sep 2014 - Aug 2018

## PRESENTATION

### DETECTING THE NOT POWERSHELL GANG

DEF CON Blue Team Village | 2020

Hackfest Quebec City | 2018

### HUNTING IMMATURITY MODEL

SANS Threat Hunting and Incident Response Summit | 2020

### CFP 101

Cyber Defender Indonesia Webcast | 2020

### HOW TO UNATT&CK YOUR ATT&CK PROGRAM

EU ATT&CK Community | 2020

### THREAT HUNTING USING AZURE AD REPORT - AZULA TOOL RELEASE

SANS Blue Team Summit | 2021

SECTOR | 2021

TexasCyberSummit | 2021

# MY RESUME ?

# HANDS ON CANVA



# APPLYING

- Update your Excel tracker with application date
- Apply only to company you want to work in (or at least interviewed with)
- Apply on their website or talent site (taleo, greenhouse, etc.)
- Utilize the “paste-able” information when doing the online application
- Tailor resume as needed, sometimes they’ll also ask for Cover Letter or Letter of Motivation
- Remember to contact or ask for reference if you have one

# THE INTERVIEW



[adult audio]

# COMMON INTERVIEW STEPS



01

## Introduction Call

HR or Recruiter

Introduction to the position, to see if you are a perfect fit. They will “verify” your resume with you.



02

## Technical Interview

Team Member/Senior Team Member

Digging deeper into your technical capability. Sometimes hands on (e.g., code). Could range from 1 – 5 interviews.

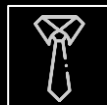


03

## Hiring Manager Interview

Hiring Manager

To see if you will be perfect fit for the team, ask question about the role, expectation, team culture, etc.



04

## Executive Interview

Director or Partner

Larger corporation started doing this, ask question about the goal of the company, company culture, or anything related to the company.



05

## Job Offer Review

Hiring Manager or HR

The meeting is to explain the terms in the job contract and to answer all your question related to that (or other left unanswered questions). Offer negotiation can happen here. Sometimes this come first before Executive interview.

# TYPE OF INTERVIEW

## **“Formality”**

Technically already got the job  
Thanks to Networking/Connections  
Ranging from 1 to 2 meetings

## **Regular**

HR -> Technical -> Hiring Manager  
followed by offer  
Ranging from 4 to 6 meetings  
Technical can be from 1 to 3 meetings

## **Technical Heavy**

A lot of technical interview, started with verbal followed with one or more hands on activity (coding, using tools, blackboard, etc.)

## **Classic FAANG**

Sometimes started with “general” Recruiter, which later connect you with specific Recruiter  
Introduction meeting with Hiring Manager  
The “Real” Interview,  
At least 1 full day  
3 to 15 different people  
At least 4 different meetings  
Touch different aspects, some behavior some technical  
They fly you to their office



# INTERVIEW TIPS & TRICK

## **STAR**

Situation, Task, Action, Result

By using this format, you will by default give the important aspect of your behavior question

## **Practice**

Practice common behavior and technical questions, role play works!

Search on Google and GitHub for common interview questions – See outro for some examples

Articulate your answers

## **Prepare Specific Scenario**

Such as projects that went well, problem with teammates, working without supervision and similar situation.

## **Ask Questions**

Interview is a 2-way communication

Company and Team culture

Day to day responsibilities

Successful candidate for the position

Management style

Performance metrics/KPI

Current goal of the team

What do you think of me so far

Training programs or budgets

How do you like the company

Talk about current news of the company

Team hangout/activity

Next steps in the interview

## **Get Ready, Even for Zoom**

Dress properly for the call, at least not in your pajamas

Dress as you are one of the employee (if in person)

## **Research**

Read the company website and news section

OSINT your interviewer to see their background, help you understand the role better too

## **Arrive early**

15 minutes for in person meeting, 5 minutes for Zoom meeting

## **Stay Calm and Focus**

Maintain eye contact, avoid looking away from camera

Pay attention to question, make sure you understand exactly what they want you to answer.

Ask them to repeat or rephrase the question if you don't understand

Take a moment of silent to think the answers instead of using filling words such as "hmm" or "uh"

## **Integrity**

It is okay to not know all the answers

Let them know if you don't know the answer and ask for the answer if possible

NEVER LIE

## **Manners**

Avoid cutting the interviewer off, especially when they are asking question or answering your questions

Don't badmouth your previous company

Respect everyone you meet

Pay attention and avoid zoning out

Smile (just enough, not too much!)

Send Thank You note (my personal view)

# INTERVIEW RESOURCE

## **TECH BEHAVIOR QUESTIONS - GITHUB**

[tech-interview-handbook](#)

## **INFOSEC TECHNICAL QUESTION - GITHUB**

[security-prince's](#)  
[tahmed11's](#)

## **@HACKS4PANKAKES' CAREER BLOG**

[tisiphone.net](#)

## **BHIS JOB HUNTING - YT**

[youtube.com](#)

## **DANIEL MIESSLER'S CAREER BLOG**

[danielmiessler.com](#)

## **DANIEL MIESSLER'S 60 TECHNICAL QS**

[danielmiessler.com](#)



BREAK TIME

# 04

## THE BALANCE

- What to do after all the process
- Keeping Physical and Mental Health in check

**WHAT'S NEXT?**



## **Learn skills that you are missing**

There will always be a free option  
Update your CV (Resume) regularly, ask for feedback!

## **Practice Interview**

You can do it with friends, family, mentor or career advisor  
Look for commonly asked question both technical and behavior

# **WAITING**

# SUCCESS 😊

- Response to the interview invitation
- Schedule the time that works for you, account travelling time too
- Interact with the recruiter to get more insider insights or anything that is unclear about the process
- Talk to people in the company e.g., via LinkedIn, Chat Group, or Meetup to understand more about the role
- Do more practice interview
- Celebrate!



It is okay, take this as a learning opportunity, review and find place to improve!

Keep contact with the people you met along the journey

Don't be sad and move to the next application ☺

**FAILED** 😞



### **Cyber Security can be harsh**

Cyber security can be technically demanding, make sure to always have fun on the side and call it a day when needed

### **Being strategic and realistic**

Don't push yourself to do a job search for too long, suggested is 2-hour period a day

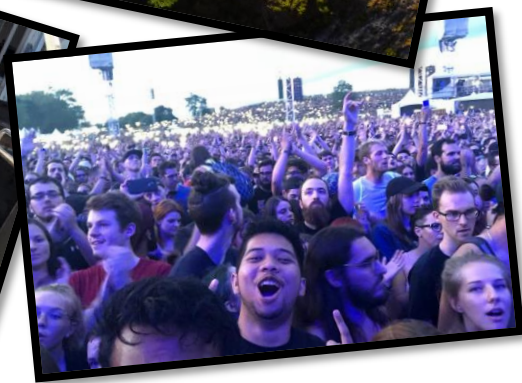
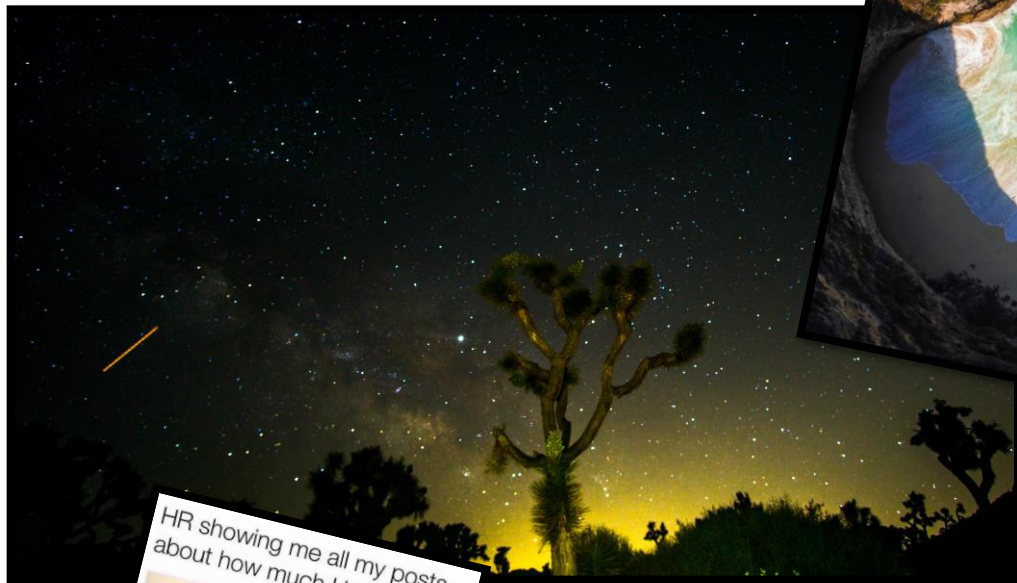
When you are tired, you won't focus, and you will make mistakes

### **Have fun, don't stress it out!**

Play games, go hiking, do other fun stuff! A hobby (or more) can help you find new perspectives and ideas

# THE BALANCE

# LIFE IS NOT JUST CYBER SECURITY



Impostor



**IMPOSTOR SYNDROME IS REAL**  
**BELIEVE IN YOURSELF!**

# 05

# CLOSING

Closing Remarks and Q&A

# PEOPLE TO FOLLOW

**KATIE NICKELS**



[LinkedIn](#)  
Threat Intelligence

**NASREDDINE BENCHERCHALI**



[LinkedIn](#)  
Threat Hunting, Detection Engineering

**BOBBY COOKE**



[LinkedIn](#)  
Red Team, Vulnerability Research

**PATRICK WARDLE**



[LinkedIn](#)  
MacOS Security

# **NEWCOMER CONFERENCES**

## **SANS NEW TO CYBER SUMMIT**

<https://www.sans.org/event/newto cyber-summit-2021>

## **PANCAKES CON**

<https://pancakescon.com/>

## **BSIDES LV – PROVING GROUND**

<https://www.bsideslv.org/proving-ground/>

# STARTING UP GUIDE

**ISSESSIONS'**  
THE WONDERFUL WORLD OF INFORMATION SECURITY

[youtube.com](https://www.youtube.com)

**AWESOME-INFOSEC**

[awesome-infosec](https://www.awesome-infosec.com)  
[awesome-security](https://www.awesome-security.com)

**INFOSEC ADVICE TWITTER THREAD**

[twitter.com/j\\_opdenakker](https://twitter.com/j_opdenakker)

**BLACK HILLS INFOSEC YT**

[youtube.com](https://www.youtube.com)

**DANIEL MIESSLER'S INFOSEC CAREER**

[danielmiessler.com](https://danielmiessler.com)

**@HACKS4PANKAKES' CAREERS AND  
EDUCATION RESOURCES**

[tisiphone.net](https://tisiphone.net)



# LOCAL CONFERENCES AND MEETUPS

## **SECTOR**

<https://sector.ca/>

## **TORONTO AREA SECURITY KLATCH (TASK)**

<https://task.to/>

## **BSIDES TORONTO**

<https://www.bsides.to.ca/>

## **HACKFEST (QC)**

<https://hackfest.ca/>

## **NORTHSEC (QC)**

<https://nsec.io/>

## **OWASP TORONTO**

[https://owasp.org/www  
-chapter-toronto/](https://owasp.org/www-chapter-toronto/)

# THANKS TO...

HOPE conference team

Resources and tools creators

People to follow connections  
(Katie, Bobby, Patrick, and Nasreddine)

Recruiter connections  
(Maite, Ricki, and Josh)

My manager & team

# THANKS

Do you have any questions?

@tas\_kmanager  
/in/tondangmangatas



CREDITS: This presentation template was created by **Slidesgo**, including icons by **Flaticon**, and infographics & images by **Freepik**.



# **SLIDEDECK & OTHER MATERIALS**

**WILL BE AVAILABLE ON MY GITHUB**

Scan barcode to visit my GitHub  
ps: promised it's not a rick roll link ☺

# Q&A

What ?

**ROLES**

**COMPANY**

Who?

How ?

**HIRING**

**INTERVIEW**

Why?