

# Skillz for Pivoting into Cloud

muteki

Unconference @ Blue Team Con 2023

# Cloud Security Jobs

- Analyst
  - Evaluate security configurations of cloud environments
- Engineer
  - Implement tooling like CSPMs (Cloud Security Posture Management), ie Wiz, Orca, Prisma Cloud
- Architect
  - Design Cloud Security solutions for given environment
- DFIR, Red Team, etc.
  - ...but make it cloud!
- ...and more

# Skills

- Willingness to learn new things
- Familiarity with APIs, HTTP requests
- Linux, comfort with command line tools
- Scripting in Bash and/or Powershell
- VMs and Containers
- Identity and Access Management, authentication flows
- Basic networking \*
- Bonus: Application development and security, code pipeline security, databases
- Bonus: container orchestration / Kubernetes

\* caveat: networking is very different in the cloud!

# Buzzwords that Matter

- Shared Security Model
- Serverless and/or Microservices
- Control/management vs. data plane
- Lift & Shift (just say NO!)

Responsibility	On-Prem	IaaS	PaaS	SaaS
Data classification & accountability				
Client & end-point protection				
Identity & access management				
Application level controls				
Network controls				
Host infrastructure				
Physical security				

Cloud Customer Cloud Provider

# Pick a Cloud, any Cloud

- Have experience with Azure AD, Windows Sysadmin, O365, Defender, InTune, etc?
  - ... pick Azure and/or M365
- Have software dev or general IT experience, or want to keep options wide open?
  - ... pick AWS
- Are you a masochist?
  - ... pick GCP!

# Resources & Certs: To cert or not to cert?

- Certs: The journey is more important than the destination:
  - Use certs to create a learning plan
  - Get as hands-on as possible!
- Recommended certs:
  - for n00bs: AWS Certified Cloud Practitioner OR Microsoft Certified: Azure Fundamentals
  - For experienced folks, pick certs closely aligned with your knowledge base, ie. Azure Security Engineer Associate, Azure Administrator Associate, AWS Solutions Architect, AWS Cloud DevOps Engineer
- Other resources:
  - ACloudGuru
  - Free videos on YouTube – ex: freecodecamp.org video guides for certs
  - AWS Free Tier – get hands-on and start building stuff
  - Attend every Cloud-focused conference talk you can find, even if you only understand 10% of it.

# General Tips & Tricks

- Be flexible and willing to learn
- Take every opportunity to learn and use cloud in your current position
- Get hands-on as much as possible, use AWS free tier!
- Network (the human kind)
- Just apply for the job, even if you feel you're underqualified

# My Path into Cloud Security

- IT Desktop Support -> O365 Support (Company A)
- Azure AD/O365 Systems Administrator
- Master's in Computer Science with projects in AWS
- As Senior Consultant (Company B):
  - XDR engineering in Azure
  - AWS Cloud Security Assessments
- As Senior Consultant (Company C):
  - Azure, GCP Cloud Security Assessments
  - Azure & GCP Assessment Tooling Development

# muteki

- GitHub: [github.com/muteki-apps](https://github.com/muteki-apps)
- Twitter: [@muteki\\_rtw](https://twitter.com/muteki_rtw)
- BlueSky: [@muteki](https://blue.ski/@muteki)
- Mastodon: [@muteki@infosec.exchange](https://mastodon.infosec.exchange/@muteki)
- LinkedIn: [linkedin.com/in/cassandray/](https://www.linkedin.com/in/cassandray/)
- [muteki.cloudsec@gmail.com](mailto:muteki.cloudsec@gmail.com)