

**SKILLS  
TO BUILD  
FOR YOUR  
CLOUD SECURITY  
CAREER**

**CASSANDRA YOUNG  
(MUTEKI)**

**BSIDES PHILLY – DECEMBER 2023**

# CASSANDRA YOUNG (MUTEKI)

- Senior Consultant,  
Cloud Technical Assessments Team  
@ CrowdStrike
- Master's of Computer Science,  
Penn Engineering  
@ the University of Pennsylvania
- Director  
@ Blue Team Village



# TECHNICAL SKILLS

## GENERAL IT/TECH

- Linux
  - Command line familiarity
- Virtualization fundamentals
  - Virtual Machines
  - Containers
- Basic networking \*:
  - Protocols, TCP/IP basics
  - Subnetting, public/private addressing, network interfaces
  - Analyzing Firewall rules

\* Caveat: Networking is applied very differently in the cloud!

# TECHNICAL SKILLS PROGRAMMATIC

- Scripting:
  - Bash
  - Powershell
  - Bonus: Python
- Network and Application connectivity:
  - Familiarity with APIs
  - HTTP requests
- Bonus: Software development and automation:
  - Git and Git implementations, ie. GitHub, BitBucket
  - Application development processes, secure coding practices
  - DevSecOps, CI/CD pipelines, Infrastructure as Code (ie. Terraform)
  - Containers, container orchestration (Kubernetes)

# TECHNICAL SKILLS SECURITY

- Identity and Access Management
  - Identity federation, SSO, MFA
  - Authentication flows and types
  - Session- and token-based authentication
- DFIR-related skills
  - Log analysis
  - SIEM / log monitoring infrastructure platforms and query languages
  - Threat hunting
- Application and code pipeline security

# CLOUD SECURITY CAREERS

## JOB EXAMPLES \*

### ENGINEER

- Conducts cloud security assessments and audits, prioritizes risks
- Implements tooling for monitoring, alerting, configures firewalls and other controls
- Evaluates and configures tooling like CSPMs (Cloud Security Posture Management), ie Wiz, Prisma Cloud
- Acts as SME for other internal teams, ie. security, developers, engineers
- Configures SIEM/logging platform solutions for cloud, configures log export

### ARCHITECT

- Develops cloud security strategy and roadmaps; assesses and approves cloud services for use
- Evaluates and recommends secure authentication and permissions processes
- Designs cloud platform structure/OUs to apply security controls, guardrails
- Advises on networking infrastructure for access to cloud resources
- Develops cloud logging export strategy

\* Caveat: We all know how inaccurate job postings are...

# CLOUD SECURITY CAREERS

## JOB EXAMPLES \*

### CONSULTING

- Conducts proactive technical assessments, identifies and reports on misconfigurations, best practices, gaps in processes and technical controls
- Required to learn new environments quickly, must be able to research and present on unfamiliar services and controls
- Other engagement types can include penetration testing, tabletop exercises, Purple Teams, Incident Response, and Threat Hunting.

### ANY... BUT MAKE IT CLOUD!

- Look for jobs that have a heavy cloud component, even if they don't have Cloud in the title.

\* Caveat: We all know how inaccurate job postings are...

# PICK A CLOUD, ANY CLOUD (OR ALL OF THEM)

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



# CERTIFICATIONS: 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 entry level certs:
  - AWS Certified Cloud Practitioner
  - Microsoft Certified: Azure Fundamentals
- Recommended advanced certs - pick certs aligned with your knowledge base:
  - Azure Security Engineer Associate, Azure Administrator Associate
  - AWS Solutions Architect, AWS Cloud DevOps Engineer
  - ...etc.
- ...or whatever your current job is willing to pay for!
- Other specific certs such as CCSP (ISC2) are “nice to have”

# CLOUD TRAINING RESOURCES

- Other resources:
  - ACloudGuru, Udemy
  - Free videos on YouTube – ex: 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.
- Misc useful links:
  - <https://github.com/iknowjason/Awesome-CloudSec-Labs>
  - <https://www.antispyontraining.com/on-demand-courses/breaching-the-cloud-w-beau-bullock/>
  - <https://www.freecodecamp.org>
  - <https://learn.microsoft.com/en-us/training/>
  - <https://aws.amazon.com/training/>
  - <https://cloud.google.com/learn/training/>

# MY PATH INTO CLOUD SECURITY

- Higher Ed – IT Support Specialist >> Systems Administrator:
  - School IT Department: IT Desktop Support, Systems Administration, O365 Support
  - Central IT: Azure AD/O365 Systems Administrator
- Consulting Firm 1 - Senior Consultant:
  - Azure Engineering for XDR service
  - AWS Cloud Security Assessments
- Consulting Firm 2 - Senior Consultant:
  - Azure, GCP Cloud Security Assessments
  - Azure & GCP Assessment Tooling Development
  - Cloud SME for Tabletops and other proactive exercises across AWS, Azure and GCP
- Master's in Computer Science (MCIT at University of Pennsylvania):
  - Master's in Computer Science using Tuition benefits
  - Took every opportunity to use AWS for class projects.
  - Independent Study on Microservices security, using AWS

# GENERAL TIPS & TRICKS

- ✓ Be flexible and willing to learn  
...take every opportunity to use cloud in your current position
- ✓ Get hands-on as much as possible  
...use AWS free tier! (GCP and Azure have options as well)
- ✓ Network!  
...get to know Cloudy folks in the field, they might be your next referral
- ✓ Just apply for the job  
...even if you feel you're underqualified

# Thank you!

Find Cassandra (muteki) at:

GitHub: [github.com/muteki-apps](https://github.com/muteki-apps)

Twitter: [@muteki\\_rtw](https://twitter.com/muteki_rtw)

BlueSky: [@muteki](https://bsky.app/profile/muteki)

Mastodon: [@muteki@infosec.exchange](https://infosec.exchange/@muteki)

LinkedIn: [linkedin.com/in/cassandray/](https://linkedin.com/in/cassandray/)

[muteki.cloudsec@gmail.com](mailto:muteki.cloudsec@gmail.com)