

Xiao He

San Francisco, CA | xiaoh.net | Email: contact@xiaoh.net

Cloud Security Manager and Security Engineer with strong communication and project management competency. Skilled in risk management, security engineering, and threat modeling. Experience with building scalable and secure cloud infrastructure. Self-starter and avid tech explorer with experience in growing startups.

Experience

Twilio Inc.

Manager, Cloud Security February 2022 to Present

- Manage Twilio's Cloud Security roadmap and build high throughput Cloud Security engineering team.
- Organize, lead and facilitate cloud security project cycle through rigorous planning, easy-to-follow checklists, and regular retrospectives.
- Help build cross-functional relationships with peer security teams and other engineering teams.
- Manage early in career, mid-career, and staff level individual contributors, hold regular career development conversations, and lead Cloud Security hiring expansion effort.

Tech Lead / Staff Cloud Security Engineer September 2021 to February 2022

- Authored and documented the revamped Twilio's Cloud Security Policy to incorporate Multi-Account strategy, Kubernetes, Infrastructure as Code(IaC), and compliance-driven requirements(HITRUST, PCI, HIPPA).
- Drove the SPIFFE/SPIRE initiative & Open Policy Agent adoption as Cloudsec anchor.
- Performed security architecture reviews on IAM, Networking, Storage, and Encryption.

Senior Cloud Security Engineer April 2020 to September 2021

- Developed AWS Organization OU management and SCP deployment via Terraform.
- Migrated all production bastion SSH access from X.509 certificate to Yubikey One-Time-Password(OTP).
- Deployed the automation framework for cloud vulnerability management initiative.
- Built out AWS new account security onboarding automation via AWS StackSets.

Cloud Security Engineer August 2018 to April 2020

- Automated detection and remediation with Step functions, Lambdas, and DynamoDB.
- Performed threat modeling, incident response, and least-privileged analysis.
- Managed bastion network and Twilio's public key infrastructure(PKI) for production access.

Kilter, Inc (acquired by Blackbaud)

Co-founder & CTO June 2016 to January 2019

- Directed technology decisions and oversaw the development of React Native mobile and web apps.
- Designed and developed native AWS cloud infrastructure with services running Golang APIs, PHP, Python, Angular5 website, and CI/CD pipeline.
- Interfaced with partners and large clients and facilitated customers' adoptions.
- Managed a full-stack engineering team and prioritized feature requests and workstreams.

Industrial Refrigeration Consortium

Lead Software Engineer April 2016 to February 2017

- Refactored legacy PHP codebase and managed MySQL database and the web server.
- Redesigned internal management system with Bootstrap and jQuery.
- Developed and maintained all IRC and HVAC&R Center websites and databases.

UW-Madison IoT Systems Research Center

Researcher September 2015 to September 2016

- Designed hardware interfaces with Arduino YUN to provide activity analytics for gyms.
- Implemented integration of Amazon Echo and Slack with AWS Lambda and webhooks.

Certifications

- Certified Information Systems Security Professional(CISSP)
- AWS Certified Security - Specialty
- AWS Solutions Architect - Associate
- AWS Certified Developer - Associate
- GIAC Security Essentials Certification(GSEC)
- AWS Cloud Practitioner

Technologies

AWS
Apache
AngularJS
Burp Suite
Docker
Metasploit
Nmap
Nginx
Node.js
React
React Native
Terraform

Blogs

Alert & Remediate AWS Cloud Misconfigurations with Step Functions

- <https://xiaoh.net/thoughts/aws/2020/11/03/Vuln-Life-Cycle.html>

Time-based Control for IAM

- <https://xiaoh.net/thoughts/aws/2021/04/19/Time-based-IAM.html>

Terraform Monitoring to Your AWS Organization SCP

- <https://xiaoh.net/thoughts/aws/2021/05/20/Monitor-AWS-SCP.html>

Languages

Python	(Proficient)
Golang	(Proficient)
PHP	(Proficient)
MySQL	(Familiar)
JavaScript	(Familiar)

Skills

- Engineering Leadership & grow highly diverse and dispersed teams
- Cloud Security Architecture Review
- Scale security through Automation & DevSecOps
- Cloud merge and acquisition(M&A) due diligence and integration
- Relationship management with subject matter specific vendors
- Contract terms negotiation