Xiao He

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

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

Skills

- Cloud Architecture Review
- Security Automation
- Security Engineering
- Threat Modeling
- DevSecOps
- Identity and Access Management
- Engineering Management
- Risk Management
- Vulnerability Management
- M&A Due Diligence
- M&A integration
- Contract Terms Negotiation
- Vendor Relationship Management

Experience

Twilio Inc.

Manager, Cloud Security February 2022 to Present

- Manage Cloudsec maturity roadmap and build foundational capabilities around assessed maturity level.
- Cultivate cross-functional relationships with peer security teams, core infrastructure teams, and product teams to unblock ongoing efforts and coordinate new initiatives.
- Develop architectural patterns around Cloud Org Structure, IAM, Service Mesh, K8s, and audit logging.
- Organize and facilitate 4-5 project deliveries per quarter through rigorous planning, easy-to-follow checklists, and regular retrospectives.
- Manage a team of 9 with junior to staff ICs with regular career conversations, and lead hiring efforts.

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

- Authored the revamped Twilio 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(OPA) adoption as Cloudsec anchor, conducting architectural reviews and threat models for Service Discovery and Communication.
- Performed security architecture reviews and threat models for IAM, Networking, Storage, and Encryption.
- Conduct risk assessments, evidence gathering, and facilitate remediations for SOC 2 and PCI DSS.

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 the Cloud Vulnerability Management initiative.
- Built out AWS new account security onboarding automation via AWS Cloudformation StackSets.

Cloud Security Engineer August 2018 to April 2020

- Automated detection and remediation with Step functions, AWS Lambda, and DynamoDB.
- Performed threat modeling, incident response, and IAM 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 of 5 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

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

Technologies

AWS
CloudFormation
Kubernetes
Metasploit
Nmap
Nginx
React Native
Terraform

Languages

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