

# Xiao He

San Francisco, CA | [xiaoh.net](http://xiaoh.net) | Email: [contact@xiaoh.net](mailto:contact@xiaoh.net)

Experienced Cloud Security Manager and Engineer with a proven track record in successfully managing geographically distributed and culturally diverse teams. Cultivating a culture of innovation while constructing engineer-friendly security solutions. Demonstrated proficiency in designing scalable and secure cloud infrastructures. Adept communicator and skilled project manager with a history of aligning security initiatives with business objectives.

## Skills

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

## Experience

- Engineering Manager, Security Engineering at Credit Karma

(Aug 2024 - present)

  - Oversee Cloud Infrastructure Security (Vulnerability Management, Container Security, Detection Engineering) and Corporate Security (Endpoint Security, Data Loss Prevention, Public Key Infrastructure).
  - Drive design and implementation of services to improve Cloud and Infrastructure security posture:
    - Automatic quarantine on data security findings
    - CI/CD pipeline security scans for Cloud Services
    - End of Life management
    - Critical CVE response playbook
    - Self-service PKI automation
  - Partner with engineering and product team leaders to develop short- and long-term security, product, and service strategies including defining quarterly OKRs, and reporting on KPIs in leadership forums.
  - Hire and mentor talented engineers across cloud and corporate security, enabling career growth.
  - Manage Cloud Security and Corporate Security vendor relationships, contract negotiation, and renewal.
- Engineering Manager, Cloud Security at Twilio

(Feb 2022 - May 2024)

  - Managed a 3-year strategic cloud security maturity roadmap aligned with business top risks and NIST CSF.
  - Oversaw Cloud Vulnerability Management program and developed capabilities for scale.
  - Cultivated cross-functional relationships with peer security teams, core infrastructure teams, and product teams to unblock ongoing efforts and coordinate new initiatives.
  - Identity and Access Management: Coordinate buy-ins and deliveries for AWS Identity Center initiative across Security, IT, and Infrastructure, successfully deploying scalable human access for all engineers.

- Hired and managed a team of 8 spread globally and mentored ICs through regular career conversations.
- Managed CloudSec and Vulnerability Management vendor relationships, contract negotiation, and renewal.
- Supported ongoing ISO27001, SOC2 Type 2, PCI, and SOX audits for the enterprise.
- Managed quarterly project lifecycle with maturity roadmap and facilitated retrospectives to promote continuous learning. We:
  - Eliminated direct SSH access across account fleets for humans with AWS System Manager.
  - Automated AWS Account Tagging with ownership and security classification.
  - Mitigated IAM privilege escalation with Sentinel policy deployment and permission boundary.
  - Leveraged AI to build generative IAM policy recommendations for engineering.
  - Supported incident response and threat detection by increasing infrastructure logging coverage and developing incident responder access to cloud assets.
  - Developed and deployed M&A runbook and automation for Cloud Security.
  - Built self-serviced WAF solution for every edge service at Twilio.

#### **Tech Lead / Staff Cloud Security Engineer at Twilio**

(Sept 2021 - Feb 2022)

- Developed cloud architectural patterns around Org Structure, IAM, Service Mesh, K8s, and audit logging.
- Authored Twilio Cloud Security Policy revisions to incorporate Multi-Account strategy, Kubernetes, Infrastructure as Code(IaC), and compliance-driven requirements(HITRUST, PCI, HIPAA).
- Performed security architecture reviews and threat models for IAM, Networking, Storage, and Encryption.
- Drove the SPIFFE/SPIRE initiative & OPA adoption from security, conducting architectural reviews and threat models for Service Discovery and Communication.
- Conduct risk assessments, evidence gathering, and facilitate remediation for SOC 2 and PCI DSS findings.
- Supported Threat Hunting, Threat Detection, and Incident Response functions.
- Mentor junior ICs on navigating larger initiatives and planning dependencies.

#### **Senior Cloud Security Engineer at Twilio**

(Apr 2020 - Sept 2021)

- Deployed 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).
- Developed automation framework and JIRA metrics for the Cloud Vulnerability Management program.
- Built out AWS new account security onboarding automation via AWS Cloudformation StackSets.
- Performed due diligence on M&A targets and facilitated cloud environment integration.
- Collaborated with senior leaders from various business units and PCI auditors on formulating and establishing the standard cloud configuration framework throughout the enterprise.

#### **Cloud Security Engineer at Twilio**

(Aug 2018 - Apr 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.
- Worked as a cross-functional partner to security champions in the cloud security domain.

#### **Co-founder & CTO at Kilter (acquired by Blackbaud)**

(June 2016 - Jan 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.

#### **Lead Software Engineer at Industrial Refrigeration Consortium**

(Apr 2016 - Feb 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.

#### **Researcher at UW-Madison IoT Systems Research Center**

(Sept 2015 - Sept 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.

## **Blogs**

---

### 3 Big Transitions to go from Tech Lead to Engineering Manager

- <https://xiaoh.net/thoughts/management/2022/04/28/Tech-Lead-To-EM.html>

### 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>

## **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