AUSTIN KING

Atlanta, GA | 740-416-5889 | austin.king@outlook.com | https://austinking.cloud

SUMMARY

Cloud security leader and practitioner with 10 years of cybersecurity experience and deep hands-on expertise implementing and operationalizing CNAPP/CSPM platforms across AWS, Azure, and GCP. Deep expertise with Wiz—covering CSPM, CWPP, DSPM, identity risk, and network exposure—across 400+ cloud accounts. Proven track record advising customers and internal stakeholders on cloud security best practices, remediating CIS, NIST, IAM, secrets, container vulnerabilities, and building dashboards to measure security posture maturity. Comfortable operating as both technical practitioner and trusted advisor translating complex cloud risk into clear, actionable guidance for engineering teams and executive stakeholders.

SKILLS

Cloud Security & CNAPP: Wiz, CSPM, CWPP, DSPM, CIEM, Identity Risk, Network Exposure, IaC Scanning, Upwind Security, CIS Benchmarks, NIST, Zero Trust

Cloud Platforms: AWS, Azure, GCP, EC2, S3, IAM, VPC, Route 53, CloudTrail, GuardDuty, Security Hub, Control Tower, Organizations, Identity Center, Defender for Cloud

SOC & SIEM: Splunk, ArcSight ESM, Logger, ArcMC, CloudTrail, AWS Config, GuardDuty, Security Hub

IaC & DevSecOps: Terraform, CloudFormation, Wiz IaC Scanning, CI/CD, Linux, Git, Docker, Kubernetes

Identity & Governance: IAM, CIEM, Okta, SSO, SAML, OIDC, AWS Identity Center, Secrets Management

Enablement & Advisory: Technical enablement programs, demos and workshops, executive-level communication, translating technical risk into business impact, vendor & partner management, cross-functional collaboration

PROFESSIONAL EXPERIENCE

MANAGER, CLOUD SECURITY INFRASTRUCTURE

Barracuda Networks | May 2023 – April 2026

- Owned and operationalized **Wiz** CNAPP as the primary cloud security platform across AWS, Azure, and GCP — **driving adoption across CSPM, CWPP, DSPM**, identity risk, network exposure, and IaC scanning
- Established risk based triage and remediation workflows that **reduced critical and high-severity findings by 75% across over 400 cloud accounts**
- Led a team of cloud security engineers managing day-to-day operations and technical direction for cloud security infrastructure across AWS, Azure, and GCP
- Implemented and expanded Wiz DSPM to identify, classify, and reduce sensitive data exposure
- Drove container and workload security visibility using Wiz CWPP, **implementing scanning for containers and Kubernetes environments**
- Assessed cloud security posture across multi-account AWS and Azure environments, **remediating CIS, NIST, and cloud-native compliance violations**

- Performed cloud entitlement reviews and IAM remediation — addressing excessive permissions, privilege escalation paths, and identity misconfigurations
- Acted as the **primary Wiz platform SME**, partnering with engineering, platform, and cloud teams to translate findings into actionable architectural guidance
- Drove internal enablement and adoption by leading "Wiz Jam Sessions", educating teams on attack paths and best practices
- Integrated Wiz security scanning into **CI/CD workflows** to identify cloud misconfigurations.
- Maintained strong partnerships with Wiz, cloud service providers, and security vendors, influencing roadmap discussions and feature adoption
- Mentored and onboarded cloud security engineers, **strengthening both technical execution and cross functional communication**

KEY PROJECTS:

- **Cloud Security Maturity Model**
  Designed and implemented an internal cloud security maturity model to assess and score business units against security best practices, establishing measurable KPIs to track progress over time.
- **Wiz Cloud Security Platform Operationalization**
  Redeployed and fully operationalized Wiz across AWS, Azure, and GCP — achieving 100% cloud asset visibility and enabling CSPM, CWPP, and DSPM from the ground up. Established risk based alerting workflows, tuned signal-to-noise across all finding categories, and drove structured remediation that reduced critical and high-severity cloud risk by 75% across 400+ accounts.

MANAGER, CLOUD & TECH OPERATIONS

Deepwatch | May 2021 – February 2023

- Owned cloud and tech operations for multi-cloud environments (AWS, Azure, GCP) while leading a fully distributed team of engineers, architects, and IT specialists supporting a national workforce
- Operationalized Wiz CSPM to improve risk visibility and remediation velocity; implemented continuous CIS Benchmark monitoring and automated security tooling
- Directed employee onboarding and offboarding, including identity provisioning/deprovisioning, access management, asset management and device readiness
- Optimized service desk operations supporting national workforce, reducing average ticket response times by 50% through process improvements, team enablement, and strategic resource allocation
- Advised business units on cloud strategy and operational best practices
- Led initiative to achieve AWS MSSP Level 1 Competency, validating cloud security maturity and strengthening customer trust
- Managed strategic vendor relationships and 24x7x365 cloud and business support model
- Recruited, mentored, and conducted performance management for distributed technical team
- Implemented cost optimization strategies and served on change advisory board (CAB) for business-critical infrastructure decisions

KEY PROJECTS:

- **AWS Control Tower Implementation**
  Designed and deployed AWS Control Tower in a multi-account environment, automating landing zones with governance guardrails, centralized logging, and Identity Center integration; improved account provisioning speed by 50%.

- **AWS MSSP L1 Competency Achievement**
  Led the cross-functional initiative to achieve AWS MSSP Level 1 Competency, coordinating technical validation, documentation, and stakeholder engagement. This achievement strengthened customer trust and validated the organization's cloud security maturity.

ARCHITECT, CLOUD & TECH OPERATIONS

Deepwatch | March 2019 – May 2021

- Architected platform monitoring and observability to improve reliability and incident response
- Architected and deployed AWS Control Tower in a multi-account environment, designing the organizational structure, OU hierarchy, SCPs, and baseline guardrails for 100+ accounts
- Implemented AWS Identity Center (SSO) integration with Okta, designing permission sets, role based access patterns, and automated user provisioning workflows
- Architected centralized logging and security monitoring solution aggregating CloudTrail, Config, GuardDuty, and Security Hub findings into S3 for integration to Splunk
- Built secure lab and sandbox environments to enable safe experimentation, cost controls, training, and cloud adoption across engineering teams
- Performed CIS Benchmark assessments across cloud workloads and identified remediation paths
- Architected and implemented 100+ Okta SAML/OIDC identity federations with customer identity providers, designing secure authentication flows and session management

SECURITY ENGINEER II

GuidePoint Security | September 2017 – March 2019

- Certified Splunk Architect leading implementation projects for 20+ enterprise customers
- Performed Splunk Enterprise upgrades across distributed environments with zero downtime
- Conducted security gap analysis and translated findings into actionable security use cases

SECURITY ENGINEER / SECURITY ANALYST

ReliaQuest | December 2015 – August 2017

- Subject matter expert in ArcSight SIEM (ESM, Logger, ArcMC, Connectors) — log source integrations, platform upgrades, technical documentation, and SOPs
- Tier 1 SOC analyst for 24/7/365 MSSP operations — security event analysis, incident response, and incident runbook development standardizing IR processes across SOC teams

CERTIFICATIONS & EDUCATION

- AWS Solutions Architect – Associate
- Professional development: Communicating Persuasively & Building Trust (Stanford GSB) · Communicating Inclusively (Ivy Academy) · Achieving Mental Flow & Thriving (Duke)
- B.S., Digital Forensics & Information Assurance — Marshall University, Huntington, WV | December 2015