AUSTIN KING

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

OVERVIEW

As an experienced information security professional, with 10 years of experience in IT, I bring a proven track record of successfully architecting, managing, and securing cloud infrastructure. I have a strong ability to communicate complex technical concepts, so audiences of all skillsets can understand. I am skilled with technical project management, communicating and building relationships, and leading distributed technical teams. I have a strong will to do the "hard right" and consistently deliver projects that exceed expectations. My passions for information security and cloud intersect nicely in the cloud security space.

SKILLS

Cloud Platforms:
AWS (EC2, S3, IAM, GuardDuty, Security Hub, VPC, Control Tower, Organizations, Identity Center, Route53), Azure (VMs, Security Center, Blob Storage, Policy, Backup, VNet), GCP (baseline experience)

Security Tools:
Wiz, CSPM, Splunk, GuardDuty, Security Hub, AWS Config, CIS Benchmarks, Zero Trust, SIEM (ArcSight, Splunk), SAML, Okta

Infrastructure & Automation:
CloudFormation, Linux, Git, monitoring (CloudWatch, Splunk), logging

Leadership & Collaboration:
Team leadership, mentoring, cross-functional collaboration, stakeholder communication, vendor management, Agile project management

Soft Skills:
Translating technical concepts for non-technical audiences, empathetic leadership, driving accountability, proactive problem-solving

PROFESSIONAL EXPERIENCE

MANAGER, CLOUD SECURITY INFRASTRUCTURE

Barracuda Networks | May 2023 – Current

- Led daily operations of the cloud security team
- Optimized and operationalized cloud security posture management using Wiz
- Developed and implemented a triage process, significantly reducing critical incidents
- Implemented data security posture management, DSPM, in a multi-cloud environment
- Ensured best practices for full visibility across AWS, Azure, and GCP cloud environments
- Participated in internal cloud working groups to promote best practices, hosting "Wiz Jam Sessions"
- Maintained robust relationships with vendors and partners
- Trained and mentored new hires on cloud security and soft skills

MANAGER, CLOUD & TECH OPERATIONS

Deepwatch | May 2021 – February 2023

- Managed the day-to-day operations of a multi-cloud environment
- Managed a fully remote, distributed team of engineers and architects
- Implemented and managed security controls for cloud environments, both detective & preventative
- Implemented automated security tooling deployment to cloud account builds; GuardDuty, Splunk
- Implemented Cloud Security Posture Management (CSPM); Wiz
- Implemented and monitored continuous CIS Benchmarking for cloud best practices for production
- Implemented cost optimization strategies across a multi-account environment
- Maintained strong relationships with vendors
- Managed a 24/7/365 cloud support model ensuring high availability of cloud platforms
- Provided cloud security best practices to various business units
- Led initiative to achieve the AWS MSSP L1 Competency certification proving proficiency on AWS
- Led and oversaw projects and proof of concepts to evaluate new technologies
- Stayed up-to-date with the latest security trends and technologies

ARCHITECT, CLOUD & TECH OPERATIONS

Deepwatch | March 2019 – May 2021

- Certified AWS Solutions Architect – Associate
- Designed and implemented a platform monitoring strategy to detect and isolate platform issues
- Implemented AWS Control Tower in our AWS Organization; including deployment of identity center
- Designed a landing zone for new account builds with guardrails, governance and logging automated
- Architected and deployed AWS lab account environments to allow teams and safe and secured account to sandbox new features and technologies; promoted a cloud first culture
- Conducted a manual (CIS) cloud assessment benchmark of production workloads
- Conducted a proof of concept with Zero Trust vendors
- Completed over 100 IdP federations between Deepwatch Okta and customer identity providers
- Created and maintain technical documentation among various systems
- Strong ability to troubleshoot system errors and reduce downtime of system availability

SECURITY ENGINEER II

GuidePoint Security & Deepwatch | September 2017 – March 2019

- Certified Splunk Architect
- Served on the implementation team with a focus on onboarding new customers
- Conducted log source integrations from various systems to Splunk Enterprise
- Deployed and maintained Splunk Enterprise in clustered and highly available environments
- Completed Splunk Enterprise upgrades; search heads, indexers, and heavy forwarders
- Completed security gap analysis for client log sources for security use case requirements
- Completed necessary technical documentation
- Participated and engaged in customer status calls and working sessions

SECURITY ENGINEER

ReliaQuest | September 2016 – August 2017

- Served as a subject matter expert in ArcSight ESM, Logger, ArcMC and Connector SIEM platform
- Performed system health checks on the ArcSight platform to ensure optimal performance
- Performed log source integrations into ArcSight SIEM to ensure visibility into customer environments
- Performed extensive ArcSight platform upgrades for all layers of the system stack
- Onboarded and integrated new customers into the security operations center for monitoring
- Developed over 50 ArcSight Flex Connectors for customers with custom log sources
- Developed technical documentation and standard operating procedures around ArcSight
- Participated in customer quarterly business reviews (QBRs)
- Served as primary engineer on Fortune 500 customers

SECURITY ANALYST

ReliaQuest | December 2015 – September 2016

- Served as a Tier 1 SOC analyst for a 24/7/365 MSSP monitoring team
- Performed security analysis alerts that were generated from various SIEM systems
- Performed log analysis from various systems that produce security related logging
- Inducted incident response on SIEM alerts and provided analysis to customers
- Developed incident run books to standardize the IR process across SOC teams

SELECTED PROJECTS

Cloud Security Maturity Model

Designed and implemented an internal cloud security maturity model to assess and score business units across cloud security best practices. Metrics includes MTTR, open incident/vulnerability counts, participation in cloud security training, and policy adherence, and general cloud security risk. Established measurable KPIs to allow teams to score and track their progress over time.

Wiz Cloud Security Platform Operationalization

Operationalized Wiz CSPM and DSPM tools across AWS, Azure, and GCP, reducing critical security misconfigurations by 30% and achieving full visibility across 100% of cloud assets.

AWS Control Tower Implementation

Designed and deployed AWS Control Tower across a multi-account environment, automating landing zone setup with governance guardrails, centralized logging, and identity center integration; improved account provisioning speed by 50%.

AWS MSSP L1 Competency Achievement

Led team initiative to achieve AWS MSSP Level 1 Competency, aligning security operations with AWS requirements; enhanced cloud security offerings and validated organizational expertise for AWS customers.

CERTIFICATIONS

- AWS Solutions Architect – Associate (License B86HW2L2KNRQ1M91)
- AWS Certified Security – Specialty (In Progress – Expected April 2023)
- Splunk Certified Architect (Cert-208562)
- Communicating Inclusively (The Ivy Academy)
- Communicating Persuasively and Budling Trust (Stanford Graduate School of Business)
- Achieving Mental Flow & Thriving (Duke Corporate Education)

EDUCATION

BACHELOR OF SCIENCE; DIGITAL FORENSICS & INFORMATION ASSURANCE

Marshall University / Huntington, WV / August 2012 – December 2015