# Amber Hart

CLOUD SECURITY ARCHITECT

**Atlanta, GA | 706.267.1100 | amberhart01@outlook.com**

## Professional Summary

Cloud Security Architect with 7+ years of experience designing and securing enterprise-grade cloud environments across industries including energy, finance, and education. Proven expertise in DevSecOps, AI-driven compliance automation, and quantum-resilient security strategies. Passionate about simplifying security operations and bridging gaps between technical teams and business stakeholders. Known for building innovative tools and leading projects from architecture through deployment with a strategic and collaborative mindset.

## Experience

**Southern Company | Cloud Security Architect** **May 2024 – Present**

- Lead cross-functional efforts to deploy Wiz across multi-cloud environments (Azure, AWS, GCP), collaborating with engineering and operations teams to integrate tooling and enforcing unified policy-as-code standards using Terraform and OPA.
- Manage enterprise wide quantum readiness efforts by maintaining a PQC roadmap, coordinating with internal stakeholders to inventory cryptographic assets, engaging vendors to evaluate post-quantum compatibility and strategic risk.
- Designed and implemented an AI-powered policy comparison tool using Azure OpenAI and LangChain to identify control gaps between Wiz and Microsoft Defender for Cloud.
- Lead strategic planning and deployment of a secure Terraform state file to support scalable IaC practices and establish standardized cloud infrastructure across the enterprise.
- Direct enterprise-wide azure gap assessment using the Microsoft Security Benchmark, identifying control gaps and coordinating remediation across technical teams.
- Advise development and operations teams on mitigating security weaknesses and identifying new solutions to enhance the organization's cloud security posture.

**TCM Bank | Application Security Engineer (Contract)** **Feb 2024 – May 2024**

- Conducted API security testing using Burp Suite and Postman prior to production deployments, identifying and mitigating critical vulnerabilities.
- Partnered with developers to triage and remediate security vulnerabilities across APIs and web applications, aligning fixes with risk severity and audit timelines.
- Authored application security policies and supporting documentation to guide secure development practices and promote consistency across teams.

**Southern New Hampshire University | Cloud Security Engineer (Contract)** **Mar 2023 – Jan 2024**

- Liaison between Office of Product Innovation and Information Security, enhancing cloud security in Azure and GCP; integrated automated security checks into GitHub Actions CI/CD pipeline**s.**
- Managed Wiz CSPM POC deployment, customizing and integrating it effectively, and communicated strategic advantages to senior leadership for seamless adoption.
- Directed GCP IAM audit and cleanup, enforced MFA, and integration of ServiceNow ticketing for centralized access requests and onboarding/offboarding. Standardized password configurations to align with university security frameworks.

- Collaborated with DevOps team using tools like CodeQL, Dependabot and Tenable WAS for proactive security vulnerability detection and remediation.
- Serve as a cloud security SME, providing architectural guidance and threat mitigation strategies across engineering, DevOps, and security teams.
- Authored secure coding policies and disaster recovery plans, guiding development teams in best practices for cloud security response strategies.

**Voice | DevSecOps Engineer** **Jan 2022 – Mar 2023**

- Leveraged SonarQube for CI/CD pipeline integration, automating code quality and security scanning, and leading collaboration for vulnerability management.
- Managed enterprise-wide vulnerability detection and mitigation with Tenable.io, integrating into CI/CD for automated security assessments.
- Implemented and managed Dependabot in GitHub Actions, automating dependency updates and integrating security into development workflows.
- Utilized Google Security Command Center for comprehensive threat detection, risk assessment, and security policy enforcement across GCP assets.
- Conducted in-depth security analysis of smart contracts using Trail of Bits tools, driving innovation in blockchain application security.
- Orchestrated Cloudflare services to enhance web security, managing DDoS mitigation, WAF configuration, and secure content delivery.

**PKM/Crowe/Coalfire | Senior IT Auditor & Security Consultant** **May 2018 – January 2022**

- Delivered 50+ IT security assessments and audits across regulated industries; evaluated IAM controls, infrastructure & cloud security, vulnerability management and SDLC risks under PCI-DSS, HITRUST, SOC 2, SOX, and GLBA.
- Supervised and mentored junior team members during IT audits, providing technical guidance, reviewing workpapers, and fostering a culture of quality, accountability, and continuous improvement.

## Projects

---

**RiskShield** - *AI Business Solution*

- Architected and developed LLM solution for reviewing security controls (NIST) using LangChain, Open AI Embeddings, GPT-4, FastAPI, HTML/CSS, Azure Web Apps, Docker, and ChromaDB.
- Streamline and automate compliance assessments by integrating LLM, document parsers and RAG to analyze security documents against compliance frameworks and draft structured compliance reports.

**Cloud Security Chatbot** - *Context-Aware Memory Chatbot*

- Built a cloud security chatbot using LangChain, Streamlit UI, VectorStoreRetrieverMemory, ConversationBufferWindowMemory and OpenAI GPT-4 to assist with posture questions and tooling guidance.
- Embedded a lightweight memory layer into an LLM-powered chatbot, enabling operators to retrieve environment facts and past resolutions instantly, saving time and reducing context-switching overhead.

**Compliance Advisor Chatbot** - *Building Domain Specific AI*

- Designed AI tool to automate compliance checks using Streamlit UI, FetcherAgent, GapAgent, Analytzer Agent, LangChain agents, ChromaVector Store, and OpenAI GPT-4.
- Compliance Advisor Chatbot is a specialized AI assistant built to help organizations compare their internal security policies against the NIST SP 800 53 standard

**Synchronizing Cyber and Political Events Across Nations** - *Three Minute Thesis: Exploring Cyber Threat Patterns as Predictive Indicators of Geopolitical Crises*

- Conducted a cross-correlation analysis using BigQuery, SQL, and Looker Studio to evaluate and visualize monthly cyber-attack volumes against global geopolitical event data.
- This cross-correlation analysis demonstrates that cyber-attack volumes not only mirror geopolitical crises but, in key cases such as Ukraine, can precede them—offering valuable early-warning signals.

## Education

**Georgia State University, Master of Business Administration** **2023 – 2026**
Computer Information Systems | AI Business Innovation Certificate

**Georgia State University, Master of Science** **2017 – 2018**
Information Systems Audit and Controls

**Georgia State University, Bachelor of Science** **2011 – 2016**
Public Policy

## Certification

**DevSecOps Masterclass** | BlackHat August 2023
**Academy Live - Mastering MITRE ATT&CK** | AttackIQ April 2023
**Certificate of Cloud Security Knowledge** | Cloud Security Alliance August 2021
**Certified Information Systems Auditor** | ISACA May 2020

## Skills

- Cloud Infrastructure Security & Architecture
- DevSecOps
- AI Infrastructure and Architecture
- Network Security
- Identity and Access Management (IAM)
- Security Compliance (e.g. GDPR, HIPAA)
- Vulnerability Management
- Encryption Technologies
- Security Automation
- Penetration Testing
- Security Information and Event Management (SIEM)
- Risk Management and Assessment
- Problem Solving and Critical Thinking
- Communication and Presentation Skills
- Collaboration and Cross-Functional Coordination
- Adaptability and Flexibility
- Time Management and Prioritization
- Leadership and Team Management
- Decision Making and Strategic Planning

## Technical Tool Kit

**Cloud Platforms/CSPM/CNAPP:** Azure, GCP, AWS, Wiz, Prisma Cloud, Microsoft Defender for Cloud, Google SCC

**DevSecOps & Application Security:** Terraform, GitHub Actions, Azure DevOps, Buildkite, SonarQube, Checkmarx, Dependabot, OPA, CodeQL, Burp Suite, Postman, Tenable, OWASP Zap, Semgrep

**AI/LLM Engineering & Web Development:** LangChain, OpenAI API (GPT-4), Agentic AI, RAG, ChromaDB, FAISS, scikit-learn, Streamlit, FastAPI, Python, HTML/CSS, Javascript

**Monitoring & SIEM:** Azure Sentinel, Splunk, Datadog

**IAM & Security Controls:** RBAC, MFA, GCP Recommender, Policy-as-Code, Azure Policy

**Security Frameworks:** NIST SP 800-53, SOC 2, HITRUST, PCI-DSS, GLBA, SOX

**Other Tools**: Docker, Cloudflare, Trail of Bits