SHAWHEEN AZIMI

Senior Security Architect, Engineer, and Analyst
shawheen56@gmail.com | linkedin.com/in/shawheen-azimi | github.com/shawheen1904

SUMMARY

Senior security engineer with experience across cybersecurity, cloud security architecture, detection engineering, incident response, and AI-enabled security operations in high-assurance environments. Combines deep technical execution with business-minded security program leadership.

PROFESSIONAL EXPERIENCE

General Atomics & Affiliated Companies
Senior Security Engineer & Architect | Oct 2025 - Present
Security Engineer - Detection & Response II | Mar 2024 - Oct 2025
Security Engineer - Detection & Response | Oct 2022 - Mar 2024
Cybersecurity Analyst | Nov 2021 - Oct 2022

Multi-Cloud Security Architecture & Governance: Owned design and build-out of enterprise cloud security programs across regulated environments, integrating cloud-native controls with existing security infrastructure to support secure workloads at scale.

Enterprise Incident Response: Served as senior incident response lead for enterprise-scale security events, coordinating containment, eradication, and executive risk communication across large endpoint environments.

Detection Engineering Platform: Architected a Detection-as-Code CI/CD platform, treating detections as software through Git-based version control, rule conversion, automated efficacy testing, and validation workflows.

Compliance Program Leadership: Led enterprise-wide CMMC readiness across security control domains, supporting evidence development, control implementation, and third-party assessment activities.

Adversary Emulation & Defensive Validation: Led adversary emulation and defensive validation exercises to improve detection coverage and control effectiveness across enterprise environments.

Digital Forensics: Directed sensitive digital forensic investigations while preserving evidentiary integrity, stakeholder coordination, and operational continuity.

AI-Powered Security Operations: Built and integrated AI-enabled workflows into security operations tooling to accelerate triage, enrichment, and investigative decision-making.

Global SaaS Security Architecture: Owned security architecture and engineering for a global SaaS platform, implementing secure-by-design cloud infrastructure, identity segmentation, and telemetry pipelines in a regulated environment.

Security Automation: Designed enterprise automation workflows for alert enrichment, investigation, and response, producing seven-figure efficiency gains and enabling continuous operations.

Threat Modeling Framework: Created a threat-modeling framework to assess cloud workloads, enterprise applications, and emerging technologies against realistic attack paths and business impact.

Security Observability Modernization: Architected a cloud-native observability platform consolidating enterprise telemetry and replacing legacy tooling while improving correlation, retention, and investigative performance.

Security Correlation Platform: Led major enterprise security platform modernization across cloud, endpoint, network, and identity telemetry to improve automated correlation and reduce manual triage.

EDUCATION

Bachelor of Science in Information Systems - San Diego State University
Academic Honors: Dean’s List | Cyber Defense Team | Association of IT Professionals

CERTIFICATIONS

Architecture & Incident Response: CISSP (Projected Q4 2026), CompTIA SecurityX (CASP+), GIAC Certified Forensic Analyst (GCFA), CompTIA CySA+
Cloud & Platform Security: AWS Certified Security - Specialty, AWS Certified Solutions Architect, Microsoft Azure Security Engineer (AZ-500)
Security Operations: security automation engineering, security analytics platform operations, network defense technologies, vulnerability scanning and analysis
Foundational Security: CompTIA Security+

TECHNICAL SKILLS

Security Platforms: DFIR, security automation, telemetry platforms, endpoint defense, network defense, web security, secure remote access
Detection Engineering: detection rule development, defensive validation, analytics engineering, adversary-informed testing
Cloud & Identity: AWS, Azure, GCP, cloud IAM, enterprise identity platforms, access governance
Containers & Virtualization: Kubernetes, Docker, Podman, VMware
Programming & Scripting: Python, Bash, PowerShell, SQL, KQL, XQL, HTML, JavaScript, CSS
AI Engineering: Claude Code, Ollama, AWS Bedrock, OpenAI Codex, LangGraph, LangChain
Operating Systems: Windows, macOS, Red Hat Enterprise Linux, Unix, Ubuntu, CentOS, Kali Linux, Parrot OS
Frameworks & Practices: MITRE ATT&CK, NIST 800 series, CMMC, FedRAMP, IaC, CI/CD, SAST, SBOM

DOMAINS OF EXPERTISE

Detection engineering & analytics | Threat modeling & attack path analysis | Incident response & digital forensics
Security architecture & design review | Security operations strategy | Threat intelligence & adversary emulation
Vulnerability & exposure management | Cloud & identity security architecture | Security automation engineering
Infrastructure & platform security | Identity & access governance | Security policy & control design | Compliance engineering | Leadership & cross-team execution

ADDITIONAL TRAINING AND ACHIEVEMENTS

SANS FOR508: Advanced Incident Response, Threat Hunting, and Digital Forensics - Challenge Coin Winner
Mandiant Academy: Linux Enterprise Incident Response
TryHackMe: ranked in the top 1%
U.S. Citizen with active security clearance; details available upon request
Languages: English fluent, Farsi/Persian fluent, Spanish elementary