ABI KHOSLA

CISSP | CISM | GPEN | GCIH

M.S CYBERSECURITY WESTERN GOVERNORS UNIVERSITY
B.B.A CYBERSECURITY UNIVERSITY OF TEXAS AT SAN ANTONIO

abikhosla@gmail.com https://www.linkedin.com/in/abikhosla San Antonio, TX

ABOUT ME

Cybersecurity engineer with 5+ years of experience building secure-by-design processes, repeatable procedures, and risk-aware engineering practices to help organizations make better security decisions. I enjoy designing systems that remain understandable, auditable, and reliable as they grow in complexity. I'm particularly interested in applying these concepts to connected products, embedded systems, and autonomous technologies.

COMPETENCIES

Security Engineering
Threat Modeling • Secure SDLC • Requirements Engineering

Risk Engineering
Exposure Management • PCI-DSS • NIST CSF

Product & Cloud Security
Azure Policy • CNAPP • Cloud Governance

Automation
Terraform • Azure DevOps • CI/CD

RECENT EXPERIENCE

Computer Services Inc.
Information Security Engineer II 2025 - Present

Enterprise Exposure Management Framework
Designed a framework inspired by CISA SSVC that augments traditional severity-based scoring with a flexible decision model evaluating attack paths, exploitability, asset reachability, and business criticality to generate actionable remediation recommendations across multiple finding sources.
Impact: Shifted strategy from relying on severity-based scoring to risk-driven prioritization, shortening the vulnerability lifecycle while enabling continuous validation and future automated remediation.

Secure CI/CD Integration
Engineered automated container security gates within Azure DevOps CI/CD pipelines by integrating image scanning, preventing deployment of container images containing High or Critical vulnerabilities.
Impact: Embedded security into the SDLC, improving collaboration with development teams and reducing production risk through earlier vulnerability detection.

Computer Services Inc.
Information Security Engineer I 2023 - 2025

Threat Modeling Framework
Built an automated threat modeling framework that combines application profiling, STRIDE analysis, and adaptive OWASP Web Security Testing Guide technique selection to tailor penetration testing based on application architecture and business risk.
Impact: Standardized security-by-design reviews, automated penetration testing guides, and improved enterprise visibility into application risk and control effectiveness.

Policy-as-Code Initiative
Engineered reusable governance controls using Azure Policy, Terraform, and Azure DevOps to automate security requirements and standardize secure cloud deployments across Azure environments.
Impact: Reduced manual governance effort while improving configuration consistency.