Gordon Young

Principal Security Engineer

Phoenix, AZ | 480-550-1348 | gordon.j.young@protonmail.com

Overview

Principal Security Architect and Engineer with 18+ years in cloud-native security architecture, DevSecOps automation, and resilient infrastructure for SaaS and mobile applications. Proven expertise in compliance automation, threat modeling, and security practices to meet privacy and security standards. Recognized for driving regulatory compliance, embedding robust security, and achieving resilience in high-tech, mission-critical environments.

Experience

Adyton PBC | Principal Security Engineer **2022 – Present**

- Led security strategy for cloud-hosted SaaS applications and mobile clients, enhancing the company's security posture.
- Increased FedRAMP and NIST 800-53 compliance from 30% to 89%, aligning with federal standards.
- Implemented Zero Trust across multi-account AWS environments, securing IAM policies and configurations.
- Collaborated with DevOps and engineering on secure coding practices to support system resilience.

Kandji, Inc | Principal Security Engineer **2021 – 2022**

- Boosted security automation by 30% through control streamlining and tool optimization.
- Developed a risk-focused monitoring framework to improve security response times.
- Directed SOC2 Type2 certification, closing compliance gaps and maintaining certification.
- Strengthened compliance program with POAM (Plan of Action and Milestones) development.

Postmates, Inc. | Principal Security Engineer **2018 – 2021**

- Boosted security automation by 30% through control streamlining and tool optimization.
- Developed a risk-focused monitoring framework to improve security response times.
- Directed SOC2 Type2 certification, closing compliance gaps and maintaining certification.
- Strengthened compliance program with POAM (Plan of Action and Milestones) development.

VGS | Lead Security Engineer **2016 – 2018**

- Automated EC2 compliance scans, decreasing vulnerabilities by over 30%.
- Integrated HashiCorp Vault with AWS IAM and Kubernetes, improving secure access and achieving PCI/SOC2 compliance.
- Established CI/CD security tests, reducing security flaws in production by 25%.
- Led security training across the company, reducing phishing risks and improving data security.

Skills & Tech

Cloud Security

- Expertise in securing cloud infrastructures (AWS, Azure, GCP) with a focus on Identity and Access Management (IAM), encryption, network segmentation, and security auditing.
- Experience with Cloud Security Posture Management (CSPM) tools (e.g., Prisma Cloud, Check Point CloudGuard, Aqua Security).
- Hands-on with cloud-native security practices: Kubernetes security, container security, and serverless architectures.
- Deep understanding of cloud services security frameworks (e.g., NIST, CIS, and AWS Well-Architected Framework).
- Implementing and managing CI/CD pipelines with secure development lifecycle integration (SAST, DAST, and RASP).

Mobile Security

- Securing mobile applications (Android/iOS) against vulnerabilities (e.g., OWASP Mobile Top 10).
- Implementing mobile device management (MDM) solutions and mobile threat defense (MTD) tools.
- Experience with app code analysis (static & dynamic) and app security testing using tools like OWASP ZAP, Burp Suite, and MobSF.
- Mobile app penetration testing and secure coding practices for mobile platforms.
- Application Security

Cloud Native Security

- Expertise in securing cloud-native applications, including microservices, APIs, and serverless functions.
- Experience implementing Web Application Firewalls (WAF) and API security practices (e.g., OAuth, OpenID Connect, JWT).
- Secure SDLC integration, threat modeling, vulnerability management, and penetration testing.
- Familiarity with DevSecOps practices and toolsets (e.g., GitLab, Jenkins, SonarQube, Aqua Security, HashiCorp Vault).
- Network Security & Threat Detection

Network Security

- Design and implementation of secure network architectures, segmentation, and secure communications (VPN, TLS, IPsec).
- In-depth experience with intrusion detection and prevention systems (IDS/IPS), firewalls, and SIEM systems (e.g., Splunk, Elastic Stack).
- Implementing Zero Trust architectures and micro-segmentation strategies.
- Incident Response & Forensics

Incident Management

- Proven track record of handling security incidents, from detection to resolution, in cloud-native and hybrid environments.
- Expertise in digital forensics, incident triage, log analysis, and identifying malicious activity in cloud and mobile environments.
- Experience with cloud logging solutions (e.g., AWS CloudTrail, Azure Monitor) and mobile device logging.

Compliance & Governance

- In-depth understanding of regulatory frameworks such as NIST-800-53, PIC, HIPAA, SOC 2, and PCI-DSS in the context of cloud and mobile applications.
- Experience with cloud compliance automation and managing security policies in compliance with industry standards.
- Familiar with security auditing tools and conducting risk assessments for cloud services and mobile platforms.

Programming & Scripting

- Proficient in Python, Go, and Bash scripting for automation, security tooling, and custom integrations.
- Knowledge of secure coding practices and experience in reviewing codebases for security vulnerabilities.
- Familiar with infrastructure-as-code (IaC) tools like Terraform and CloudFormation for secure cloud provisioning.

Collaboration & Leadership

- Strong communication and collaboration skills, working closely with development, DevOps, and IT teams to implement security best practices.
- Leadership experience in mentoring junior engineers, conducting security training, and contributing to organizational security policies.

Certifications

- CISSP: ISC2 Certified Information Systems Security Professional #421698
- Google Cloud Security Engineer
- Thales HSM Professional

Education

Bachelor of Science in Information Systems

Davenport University, Grand Rapids, MI **2001**