Wendy Segura

linkedin.com/wendy-segura | http://github.com/wendysegura

Core Competencies

Security Governance, Risk and Compliance (GRC)
ISO 27001, SOC 1 & 2, PCI Audit Management
Policy and Procedure Creation, Review and Implementation
Management and Risk Assessments

Identity and Access Management
Security Awareness Training
Stakeholder Engagement Third Party Risk
Coding and Automation (e.g., Python, Bash)

Technology Work Experience

SECURITY ANALYST/SECURITY ENGINEER/APPLICATION SECURITY

Sage Intacct | Sage Global | Remote | 2020 - Present

AI & Data Platform Security

- Led security engineering for Sage's AI product infrastructure, including secure cloud architecture design, platform hardening, and compliance readiness for emerging AI services
- Reviewed data dictionary sets for new AI initiatives tied to Sage Intacct, ensuring proper data classification, governance standards, and secure-by-design implementation aligned with evolving AI regulatory frameworks
- Conducted SageAI firewall reviews and created Python automation script that captures snapshots of current firewall rules and performs quarterly diff analysis, including Kubernetes Network Policy and Ingress rules reviews for SOC 2 audit compliance
- Managed vulnerability remediation in CI/CD pipelines for SageAI, partnering with Cloud Ops to ensure timely resolution and exception handling for false positives

DevSecOps & Secure-by-Design Leadership

- Embedded secure-by-design and secure-by-default principles across North American products through comprehensive threat modeling, identifying risks and driving security controls from inception to production
- Implemented and optimized security controls across CI/CD pipelines and cloud environments by onboarding products into Aqua Security (CSPM & Workload Protection), enterprise EDR, and cloud security tooling
- Conducted secure release readiness reviews, ensuring all required security controls and assessments were complete before approving features for production deployment
- Created "golden" images by leading CIS Benchmarks security assessments for Intacct, determining appropriate remediation tactics, engaging cross-team stakeholders, and validating compliance

Security Program & Compliance Management

- Managed Security GRC program including control and policy evidence generation, collection, and stakeholder engagement for PCI, SOC 1 & 2, and ISO 27001 certifications, ensuring ongoing compliance and continuous control maturity improvement
- Deployed and maintained technical security tooling including vulnerability scanning and analysis from Nessus, Palo Alto Networks, and Prisma Cloud
- Led TLS deprecation project across all Sage domains, eliminating TLS 1.0 and 1.1 support and demonstrating security program milestone delivery
- Improved enterprise security posture by remediating misconfigurations and domain vulnerabilities across BitSight monitoring
- Created Disaster Recovery checklist template based on SLAs and security policies

Cross-Functional Leadership & Team Development

- Developing DevOps team building and leadership conference for 2026, fostering community and advancing DevSecOps practices across the organization

Wendy Segura

linkedin.com/wendy-segura | http://github.com/wendysegura

- Managed Marketplace Partner security posture reviews, collaborating with Marketplace, Product, Legal, and Engineering teams to evaluate risk and negotiate mitigation strategies
- Led vendor due diligence and security risk assessments for 200+ vendors for Intacct
- Created, led, and maintained annual security awareness training for 900+ employees, including completion tracking and stakeholder engagement
- Ensured Corporate Policies were reviewed annually with stakeholders, maintaining security standards and best practices across the Intacct organization

CLOUD SECURITY ENGINEER, FELLOW

Agari | San Mateo, CA | 08/2018 – 01/2019

- Created an automated script using Lambda, and Tenable Python SDK to scan internal AWS EC2 instances and email a report to the security team upon completion
- Audited all AWS accounts IAM user groups, roles, and policies against the current access scheme to ensure Least Privilege is enforced
- Managed onboarding and offboarding by disabling access as appropriate and creating a group for IAM users no longer active with the company for monitoring purposes
- Audited IAM users for MFA authorization through Amazon's CLI to enhance security and enforce corporate requirements to use MFA
- Audited GitHub for any secrets revealed, such as key access and secret keys, using Git-Secrets and TruffleHog to ensure there were no internal passwords available to the public through GitHub

DOMAIN NAME STRATEGY SPECIALIST

CSC Corporate Domains | Los Angeles, CA | 2005 – 2006

- Analyzed methods to increase productivity and efficiency in managing client domain name portfolios
- Developed strong rapport with internet domain registries worldwide
- Exceeded domain name registration and transfer quota

PARALEGAL PROCESS SPECIALIST

CT Corporation | Los Angeles, CA | 2006 – 2010

- Managed legal document review and processing workflows ensuring organizational compliance with Secretary of State requirements
- Established quality assurance processes to ensure precise execution of client-specific legal handling requirements
- Developed and implemented team-building initiatives that improved departmental collaboration and goal achievement

Education

- Georgia Institute of Technology | *M.S., Cybersecurity Policy* | Expected 2026
- Merritt College | *A.S., Application Security*
- DeVry University | *B.S., Business Administration*
- Cerritos College | *A.A., English Literature*

Technical Publications

- Launching a Tenable Nessus Scan on an EC2
- How to use TruffleHog and Git Secrets
- Auditing your IAM users in your AWS account
- What is the difference between a hard link and a symbolic link?