**James T. Stephens**

Sparta, NC 28765 | (704) 491-3693 | [phalanx130@gmail.com](mailto:phalanx130@gmail.com) | [LinkedIn](https://www.linkedin.com/in/jameststephens/)

**CYBERSECURITY PROFESSIONAL**

Results-driven IT Operations Leader transitioning to cybersecurity with 9+ years of hands-on experience in vulnerability management, incident response, and regulatory compliance at Wells Fargo. Proven expertise in securing enterprise applications, managing security monitoring across hybrid cloud environments, and leading cross-functional teams through critical security incidents. Currently completing Google Cybersecurity Professional Certificate to formalize security expertise and transition into dedicated cybersecurity roles.

**CORE SECURITY COMPETENCIES**

* **Security Operations:** Vulnerability Assessment & Remediation, Security Monitoring, Incident Response, Risk Assessment, Threat Detection, Security Auditing, Compliance Management, Identity & Access Management
* **Technical Expertise:** SIEM Implementation, Security Automation, PowerShell Security Scripting, Network Security, Cloud Security (Azure/Hybrid), Database Security, Application Security Testing, Security Configuration Management
* **Regulatory & Compliance:** SOX Compliance, Financial Services Regulations, Security Standards Implementation, Risk Mitigation Strategies, Security Documentation, Audit Support, Change Management Security Controls
* **Leadership & Strategy:** Cross-functional Security Team Leadership, Security Project Management, Crisis Response Coordination, Security Training & Mentoring, Stakeholder Communication, Security Process Improvement

**SECURITY-FOCUSED ACHIEVEMENTS**

* **Vulnerability Management Leadership:** Directed remediation of critical security vulnerabilities across 18 applications spanning 231 servers, reducing organizational security exposure and enabling enterprise Site Reliability Engineering program launch
* **Security Monitoring Optimization:** Led initiative that reduced security alert noise by 25%, enhanced threat detection accuracy, and optimized alert routing to enterprise incident management systems, improving security team response efficiency
* **Identity & Access Security:** Architected and implemented secure Active Directory infrastructure for 52 applications during major database migration, creating 572 AD groups with appropriate security controls and least-privilege access principles
* **Security Automation:** Developed PowerShell-based security monitoring and alerting systems for enterprise applications, data feeds, and infrastructure, automating threat detection and reducing manual security oversight gaps
* **Incident Response Excellence:** Coordinated enterprise security initiatives including quarterly security reviews, monthly incident response exercises, and cross-team security drills, significantly improving organizational security posture and incident response capabilities

**PROFESSIONAL EXPERIENCE**

**Wells Fargo** | Charlotte, NC  
**Lead Systems Operations Engineer** | Jun 2023 - Present

Provide security-focused operations support for large-scale application portfolio consisting of hybrid cloud and traditional on-premises environments. Ensure compliance with cybersecurity standards, regulatory requirements, and security service level agreements through collaboration with security teams and stakeholders.

* Applied comprehensive expertise in Security Incident Management, Security Problem Management, Root Cause Analysis, Security Change Management, and Vulnerability Management to uphold Wells Fargo's technology security control standards
* Collaborated with security teams, application teams, and security tool teams to maintain Wells Fargo standards for application security observability and threat detection
* Ensured secure deployment of new security models and workflows by maintaining technical security process controls and regulatory compliance standards
* Managed ServiceNow security change management process by conducting security risk assessments, evaluating security impact, and executing security-focused approval decisions while ensuring organizational security compliance
* Analyzed security implementation feasibility of proposed changes, reviewing security validation procedures, security rollback strategies, and timelines to minimize security risks and maintain system security integrity

**Senior Systems Operations Engineer** | Jun 2018 - Jun 2023

Provided Level 2 security support for portfolio of 122 cloud and server-based applications, maintaining security service level agreements and regulatory compliance. Served as Senior Security Change Manager, evaluating change requests for security compliance and risk assessment.

* Evaluated and approved security change requests as Senior Security Change Manager, ensuring adherence to security standards and providing security guidance to support teams and other organizational units
* Led security-focused team of engineers to identify, install, and configure application security monitoring engines across 18 applications with 231 servers, eliminating critical security monitoring gaps and facilitating Site Reliability Engineering security integration
* Assessed, planned, coordinated, and scheduled middleware security vulnerability remediation across supported applications, ensuring compliance with security policies and risk mitigation requirements, enhancing overall system security posture
* Provided interim security-aware team leadership for 8-member Support group, maintaining security standards and incident response capabilities

**Systems Support Analyst** | Jun 2016 - Jun 2018

Extended security-focused SME support for 25 Azure cloud and Microsoft SQL-based applications, maintaining security uptime agreements and providing security-conscious technical assistance to customers and business units.

* Administered secure Active Directory access using multiple Wells Fargo security tools, managing user accounts, security groups, and service accounts with appropriate security controls for supported applications
* Conducted in-depth security research into data security issues affecting various business lines through SQL analysis and application security interfaces, recommending security-focused solutions that improved overall security efficiency
* Led secure Active Directory component of application database migration initiative, implementing security best practices for 572 new AD groups and SQL security role assignments for 52 applications transitioning to Microsoft SQL with appropriate security controls

**Duke Energy** | Charlotte, NC  
**Smart Grid Application Support Analyst** | May 2014 - Jun 2017

Managed application security, administered Active Directory security groups, and conducted security vulnerability reviews while maintaining compliance with Duke Energy's IT security standards.

* Contributed to the security and sustainment of 12 meter reading systems across six-state area responsible for $8.8B in annual revenue, ensuring system security and operational integrity
* Maintained security for five Load Control Systems utilized by Duke Energy's demand side management functions, implementing security controls across six-state region
* Performed security vulnerability assessments and security compliance reviews to maintain Duke Energy IT security standards and regulatory requirements

**EDUCATION & CERTIFICATIONS**

* **Google Cybersecurity Professional Certificate** - Coursera (October 2025)
* **Certified in Cybersecurity** - (ISC)2
* **AZ-900 Microsoft Azure Fundamentals** - Microsoft
* **IT Major Incident Management Professional** - MIM®
* **Splunk 7.x Fundamentals Part 1** - Splunk
* **CloudU Certification** - Rackspace Technology

**TECHNICAL SECURITY SKILLS**

* **Security Tools:** Splunk, ServiceNow Security, PowerShell Security Automation, Active Directory Security, Microsoft Security Suite
* **Cloud Security:** Azure Security, Hybrid Cloud Security, Identity Management, Cloud Compliance
* **Database Security:** Microsoft SQL Server Security, T-SQL Security, Database Access Controls
* **Security Frameworks:** Risk Assessment, Vulnerability Management, Incident Response, Security Monitoring, Compliance Auditing