# Scott Dowling

Woodstock, GA | 615.260.9549 | scott@scottdowl.ing
https://linkedin.com/in/scottpdowling

## Profile

Information Security leader with extensive experience in the Federal Reserve System, specializing in application security, vulnerability management, and security data analytics. Proven track record of uncovering and escalating critical risks to executive leadership, influencing cloud security policy, and driving compliance with regulatory frameworks. Skilled in architecting automation solutions and modernizing analytics pipelines, saving 5–10 hours weekly in reporting cycles and enabling actionable insights for remediation and risk management. Adept at bridging technical depth with strategic communication, partnering across engineering, remediation, and officer-level stakeholders to strengthen enterprise security posture.

## Skills & Abilities

### Security & Compliance

- Application Security
- Vulnerability Management
- Penetration Testing
- Risk Assessment
- Regulatory Frameworks: NIST, ISO 27001, Federal Reserve Information Security Standards (FRISS), Security Assurance for the Federal Reserve (SAFR)
- Executive Briefings & Risk Communication

### Automation & Scripting

- PowerShell, Python, SQL, Terraform, APIs
- CI/CD Pipeline Integration
- Custom Compliance & Configuration Check Tools
- Automated Patch & Health Status Monitoring

### Data Analytics & Engineering

- Tableau, Databricks, Redshift, Athena, Microsoft SQL Server
- ETL Development, Database Management, Data Visualization

### Cloud & Infrastructure

- AWS Certified Cloud Practitioner
- Secure API Development, Middleware Security, Windows Server Administration
- Cloud Security Assessments & Configuration Baselines

## Certifications

- AWS Certified Cloud Practitioner
- Data Science and Analytics Certificate – Georgia Tech

## Experience

### Federal Reserve Bank of Richmond – Information Security Advisor (09/2021 – 11/2025)

- Identified a misconfigured Databricks installation in production and development environments that allowed unauthorized root shell access, uncovering a critical privilege escalation risk with enterprise-wide impact.
- Partnered with remediation teams in technical discussions to guide secure configuration changes, ensuring alignment with Federal Reserve security standards and reducing audit exposure.
- Escalated findings to the Assistant Vice President (AVP), driving executive-level visibility into cloud security risks and influencing adoption of stricter configuration baselines and monitoring controls across multiple environments.

### Federal Reserve Bank of Atlanta – Sr. Information Security Engineer (10/2017 – 09/2021)

- Introduced Tableau to a newly formed security analytics team, establishing the foundation for enterprise-wide security data visualization and enabling leadership to monitor vulnerabilities and compliance trends in real time.
- Migrated automated reporting from Excel-based retention into a Microsoft SQL database, creating a scalable data warehouse that integrated seamlessly with Tableau and supported more verbose, actionable security reporting.
- Improved reporting accuracy and timeliness, saving 5-10 hours of manual data preparation weekly, while empowering stakeholders with interactive dashboards that informed remediation priorities and executive decision-making.

## Federal Reserve Bank of Atlanta – Sr. Systems Administrator (06/2013 – 10/2017)

- Developed multiple PowerShell automation tools to perform compliance and configuration checks against standardized security checklists, reducing manual audit preparation and ensuring consistent adherence to enterprise security policies.
- Led a patch redemption initiative for 6 appliances and 30 TV display endpoints across the bank, creating a custom PowerShell script that identified host software versions and performed real-time health status checks during upgrades, ensuring smooth deployment and minimizing downtime.
- Improved patch compliance and operational efficiency by automating vulnerability detection and remediation tracking, reducing manual intervention and strengthening overall system resilience.

## Celerant Technology – Sr. Web Developer (06/2012 – 02/2013)

- Enhanced the security of existing web applications by integrating secure coding practices and performing vulnerability assessments on client applications.
- Served as the primary point of contact for security incidents involving web applications, leading remediation efforts.

## Capital Transportation Solutions – Software Engineer (09/2010 – 06/2012)

- Developed secure APIs for logistics applications, ensuring that all data transfers were encrypted and met security protocols.
- Worked with clients to ensure that software solutions adhered to industry standards for security and usability.