

# KEVIN STALLARD

Chief Technology Officer | Chief Information Security Officer

Kennesaw, GA | 404-895-1313 | [kstallard@gmail.com](mailto:kstallard@gmail.com) | [linkedin.com/in/kstallard](https://linkedin.com/in/kstallard)

## EXECUTIVE SUMMARY

---

Technology executive with 38 years driving security transformation across gaming, financial services, healthcare, federal government, and telecommunications. Successfully built AI-powered security platforms as founding CTO while overseeing enterprise security operations with 100,000+ endpoints and \$20M budgets. Combines strategic vision with hands-on technical expertise to deliver measurable business results. Active contributor to cybersecurity policy, including Safe Harbor legislation advocacy with state legislators.

## KEY ACHIEVEMENTS

---

- Executive Leadership: Directed AI security strategy at Microsoft during \$69B Activision acquisition covering 35 game studios and 100,000+ devices across 5 major cloud platforms
- Product Innovation: Founded and created enterprise cybersecurity software platforms (EDDi compliance intelligence system, VoteSecured election security) serving healthcare, government, and financial sectors
- Quantifiable Impact: Delivered 85% reduction in security incidents, 99.92% decrease in vulnerabilities, 70% infrastructure cost savings, and 80% faster audit preparation
- Crisis Response: Coordinated global cybersecurity response during CDC Ebola outbreak across 75+ countries, collaborating with CIA, FBI, DIA, and Scotland Yard
- Patent Portfolio: Inventor on 3 approved patents covering fintech, gaming, and information security technologies; 13 additional patents pending
- Policy Advocacy: Active engagement with Georgia state legislators on cybersecurity Safe Harbor legislation

## PROFESSIONAL EXPERIENCE

---

### Founder & Chief Technology Officer

*Threat Tape LLC* | Atlanta, GA | January 2024 – Present

Founded cybersecurity consulting firm specializing in AI-powered security solutions. Serve as sole technical architect designing and building multiple enterprise software platforms from initial concept through production deployment. Direct all technology strategy, software development, cloud infrastructure, and automated deployment processes.

### *EDDi Cybersecurity Intelligence Platform:*

- Designed enterprise software platform that automatically tracks compliance requirements, assesses security risks, and provides executive dashboards for healthcare, government, and financial services organizations
- Engineered 1.77M+ line software system using modern web technologies (TypeScript, React, Next.js, Node.js) with 10+ independent microservice components
- Automated compliance monitoring for 8 major frameworks: CIS Controls, ISO 27001, FedRAMP, CMMC, SOC 2, HIPAA, NIST CSF, and PCI DSS
- Achieved 80% time reduction in audit preparation by replacing manual spreadsheet tracking with automated compliance reporting and historical trend analysis
- Implemented multi-database architecture (Amazon DynamoDB, Microsoft SQL Server, Redis) enabling sub-2-second dashboard loads at enterprise scale

- Secured Zambian government contract requiring Azure migration and ZDPA (Zambia Data Protection Act) compliance implementation

#### ***VoteSecured Election Security Platform:***

- Created comprehensive election security platform providing real-time monitoring, threat detection, and incident response capabilities to protect democratic voting processes
- Developed full-stack application using React and cloud-native architecture with blockchain-based audit trails
- Incorporated AI-powered pattern recognition, secure voter registration validation, and zero-knowledge proof identity verification
- Designed system architecture targeting 40-50% cost savings over incumbent vendors (ES&S, Dominion, Broadridge)

#### ***Cloud Infrastructure & Cost Optimization:***

- Delivered 70% cost reduction by redesigning AWS infrastructure, migrating from Kubernetes to AWS Fargate serverless computing
- Established Infrastructure as Code practices (Terraform) and containerized deployment pipelines (Docker)
- Instituted enterprise development standards including automated testing (Jest, Playwright), security scanning, and code quality requirements

### **Director of Security Architecture**

*Microsoft / Activision Blizzard King* | Atlanta, GA | June 2022 – December 2024

- Spearheaded AI security strategy for major gaming franchises (Call of Duty, World of Warcraft, Diablo), evaluating risk profiles, identifying attack surfaces, and strengthening access control mechanisms
- Oversaw 100,000+ endpoints across 5 major cloud platforms (AWS, Azure, Google Cloud, Oracle, OpenStack) with \$20M annual budget
- Orchestrated identity management (IAM) and network integration across 35 game studios during \$69B acquisition, unifying disparate security systems
- Supervised team of 6 senior security architects using servant leadership principles, improving both retention and performance
- Standardized Zero Trust security model and automated security operations through continuous deployment pipelines across all cloud platforms
- Reduced MTTR by 40% through standardized incident response procedures and automated remediation workflows
- Built GPU-accelerated CI/CD pipelines supporting game development security requirements

### **Associate Vice President, Security Architecture**

*U.S. Bank* | Atlanta, GA | March 2015 – June 2022

- Established threat intelligence program and threat hunting team utilizing AI and machine learning tools across 12 international offices to proactively identify security risks
- Chaired Security Control Review Board providing oversight for 1,500+ business applications, ensuring security standards and regulatory compliance
- Streamlined audit preparation effort by 40% across OCC, FDIC, and international regulatory examinations
- Reduced critical vulnerabilities by 35% through process automation and comprehensive security hardening of cloud-based business applications (Salesforce, Workday, ServiceNow)
- Integrated security practices into agile software development workflows, embedding automated security testing into deployment pipelines

- Developed cloud-native security dashboards and governance models for enterprise SaaS platforms

## **Owner / Chief Information Security Officer**

*GFR Technologies* | Kennesaw, GA | January 2012 – February 2015

- Directed malware analysis and system recovery operations for CDC's global cyber response during Ebola outbreak, protecting critical health infrastructure across 75+ countries
- Partnered with CIA, FBI, DIA, Scotland Yard, and international law enforcement agencies to coordinate incident response and threat mitigation
- Generated 85% reduction in security incidents and 99.92% decrease in vulnerabilities for healthcare clients through comprehensive security program implementation
- Prepared organization for DIACAP audit (Department of Defense Information Assurance Certification) from zero baseline readiness in 18 months
- Transformed proposal and RFP processes through automation, decreasing delivery time by 96% from 6 weeks to 2 days
- Served as expert witness providing technical testimony in multiple patent litigation cases

## **Senior Security Engineer**

*Northrop Grumman (Contractor to CDC)* | Atlanta, GA | 2007 – 2012

- Administered CDC's Secure Data Network identity and access management systems, ensuring compliance with federal FISMA and healthcare HIPAA regulations
- Monitored compliance using NIST 800-53 frameworks across public health information infrastructure
- Contributed to disaster recovery planning and business continuity for critical health systems
- Supported security operations for global disease surveillance and response systems

## **Senior Abuse Engineer**

*EarthLink* | Atlanta, GA | 2004 – 2007

- Prevented \$45M in fraud losses through CAPTCHA implementation across customer portals
- Reduced spam complaints by 90% through feedback loop and abuse systems redesign
- Led threat intelligence initiatives resulting in key federal convictions under CAN-SPAM Act
- Developed automated abuse detection and response systems for large-scale ISP operations

## **Build & Test Lab Manager**

*Lancope (acquired by Cisco)* | Alpharetta, GA | 2004

- Accelerated StealthWatch security product build processes, reducing time from 3 hours to 30 minutes through automation
- Supported Common Criteria certification readiness and product QA pipeline
- Integrated security product testing with CheckPoint and ISS RealSecure platforms

## **Tools & Automation Manager / Software Engineer**

*IBM / Internet Security Systems (ISS)* | Atlanta, GA | 1998 – 2001

- Revolutionized software build pipeline reducing compilation times by 97% (6 hours to 10 minutes) using Perl/XML automation
- Contributed to RealSecure platform development, winner of Network Magazine Product of the Year (1999, 2000)
- Developed dev/ops systems and tooling for enterprise security software development

## **Network Systems Engineer**

*AirTouch Cellular (now Verizon Wireless)* | Atlanta, GA | 1996 – 1998

- Supported enterprise IT systems across 600+ users in wireless telecommunications environment
- Built the first operating intranet for AirTouch Cellular providing real-time engineering metrics and tower telemetry visualization
- Implemented network monitoring and management systems for cellular infrastructure

## **Systems Administrator / Network Admin**

*Internet Systems of Atlanta* | Atlanta, GA | 1994 – 1996

- Maintained dial-up ISP infrastructure including mail, RADIUS, USENET, and Gopher servers
- Developed anti-abuse and spam mitigation policies for early ISP security operations
- Supported customer connectivity and network operations for regional internet service provider

## **Lab Assistant**

*Georgia Tech – Office of Information Technology* | Atlanta, GA | 1991 – 1994

- Maintained NeXT, Sun, Linux, Windows, and Mac systems in university computing environment
- Built Georgia Tech's first student-run web server, contributing to early Internet growth on campus
- Supported academic computing infrastructure and student technology services

## **Earlier Career**

*Various Positions* | Atlanta Metro Area | 1988 – 1991

Began technology career in 1988 with foundational roles in IT support and systems administration, building expertise that would lead to specialization in information security.

---

## **CORE COMPETENCIES**

### **Security Leadership:**

Zero Trust Architecture, AI/ML Security, Cloud Security, Incident Response, Risk Management, Threat Intelligence, DevSecOps, Election Security, Compliance Automation, Security Program Development

### **Cloud & Infrastructure:**

Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP), Multi-Cloud Strategy, Kubernetes, Docker, Terraform, Microservices Architecture, Serverless Computing

### **Programming & AI:**

Python, TypeScript, JavaScript, React, Node.js, Full-Stack Development, Machine Learning, AI Integration, LangChain, Process Automation, CI/CD Pipeline Development

### **Security Tools:**

Splunk, SIEM Platforms, Vulnerability Management, Identity & Access Management, Okta, Azure Active Directory, Penetration Testing, Malware Analysis, Threat Hunting

### **Compliance Frameworks:**

FedRAMP, PCI-DSS, FISMA, GDPR, SOX, HIPAA, NIST Standards (800-53, 800-171, CSF), ISO 27001, CIS Controls, CMMC, SOC 2, DIACAP

---

## **EDUCATION & CERTIFICATIONS**

### **Bachelor of Science, Information and Computer Science**

Kennesaw State University (degree completion) / Georgia Institute of Technology (initial coursework)

*Specialization: Organizational Management and Business Law*

## **Professional Certifications:**

- CISSP – Certified Information Systems Security Professional
- CISM – Certified Information Security Manager
- CBP – Certified Blockchain Professional

## **PATENTS & INTELLECTUAL PROPERTY**

---

- 3 approved patents covering fintech, gaming, and information security technologies
- 13 patents pending in authentication systems, secure voting platforms, and AI safety mechanisms
- Patent portfolio spans biometric authentication, blockchain-based voting, and threat detection systems

## **PROFESSIONAL ACHIEVEMENTS & ADVISORY ROLES**

---

- Technical Advisor: White-hat hacker perspective consultant to NYT Bestselling author Christie Golden on 'Assassin's Creed: Heresy'
- Expert Witness: Technical testimony in multiple high-stakes patent litigation cases
- Policy Advocacy: Active engagement with Georgia state legislators (including Todd Jones) on cybersecurity Safe Harbor legislation; consultation with Taft Law attorneys
- Dragon Con Video Gaming Track Director: Nearly 20 years (2003-2022) organizing 65+ hours of programming annually for 85,000+ attendees, featuring industry guests from Blizzard, BioWare, Epic Games, and Sony
- Nerd Gras Convention: Co-founder of gaming-focused convention in Atlanta
- EC-Council Global CISO Forum: Featured podcast guest on Application Security
- ISSA Atlanta Chapter: Board Member (2014)
- Kaspersky Partner Advisory Council: Industry representative
- SIEGE Conference Speaker: Regular presenter on security topics
- Innovation Pioneer: Created Georgia Tech's first student-run web server (1991)

## **PROFESSIONAL ASSOCIATIONS**

---

ISACA | InfraGard | CISO Executive Network | FS-ISAC | USENIX | MAAWG | ISSA