K.C. Yerrid

Melissa, TX • kyerrid@gmail.com • (704) 980-9734 • LinkedIn • GitHub

Director-level information security executive with 10+ years of architecting and executing on enterprise-wide security, strategy, and risk management for a wide range of clients, including Fortune 10 and high-growth technology organizations. Led multiple SOC transformations and high-stakes incident response initiatives—including the containment of advanced cybercriminal syndicates and the introduction of NIST-aligned playbooks and processes that reduced Mean Time to Resolution by as much as 78%. Built and scaled high-performing teams with clear KPIs and career paths, driving accountability and continuous improvement. Deep expertise in cloud/SaaS security, compliance frameworks (SOC 2, ISO 27001, PCI-DSS, HIPAA), and AI-driven threat detection to strengthen resilience and trust. Creator/Developer of CIPHER, SCOUT, and ITIDs.

CORE COMPETENCIES

Leadership & Governance: Information Security Leadership, Executive Communication, Team Leadership & Development, Cross-functional collaboration.

Security Programs & Compliance: Security Program Development, Risk Management, Compliance Frameworks, Regulatory Alignment, PCI, HITRUST, SOC2.

Security Technologies & Tools: Microsoft Sentinel, Splunk, Wazuh, Palo Alto Cortex and XSIAM, CrowdStrike, Microsoft Defender, Abnormal, Proofpoint, Zscaler, Cisco Umbrella, Wiz, FIligran OpenCTI, MISP, Velociraptor, Kape, Autopsy, FLARE, SIFT Workstation, REMNux, Kali, Burp Suite, GitHub, PagerDuty,

EXPERIENCE

Information Security Operations Manager, loanDepot – Plano, TX 09/2023 – Present

Senior-most cybersecurity operations executive leading a hybrid Security Operations Center and a team of Level 1 and Level 2 Security Operations analysts, and a team of Level 3 incident responders.

- Led the containment, eradication, and recovery efforts for an enterprise ransomware incident attributed to [redacted] using the [redacted] ransomware kit to impact the operating environment, aligning legal, privacy, and IT leadership through executive briefings and stakeholder coordination.
- Authored the organization’s Cybersecurity Incident Response Plan, aligning the document to NIST CSF v2 and NIST SP800-61r3 compliance frameworks.
- Developed incident triage protocols and a four-tier incident classification taxonomy (ITIDs), reducing response metrics (MTTA/MTTD/MTTR) by 78% in three months.
- Transformed loanDepot’s Security Operations operating model from full in-house to hybrid model by partnering with MSSP in 30 days.
- Developed a cyber threat intelligence personal knowledge management system (CIPHER) that uses YAML and Markdown languages to track observables pertaining to Cyber Threat Intelligence.
- CURRENT PROJECT: Authoring a Security Operations cockpit for cyber analysts to collect, manage, and disseminate information related to Security Operations, Incident Response, Cyber Threat Intelligence, and Cyber Threat Hunting (SCOUT).

Adjunct Instructor, ThriveDX – Remote 10/2020 – 02/2025

Taught continuing education students in advanced information security concepts, blending theory, practical labs, and interactive presentations to equip them with industry-relevant skills.

- Selected as a senior industry practitioner to deliver advanced cybersecurity education for mid-career professional and emerging leaders in information security.
- Led graduate-level instruction in Digital Forensics & Incident Response, Security Operations, Python Automation, Game Theory, and Cloud Security.
- Designed and executed immersive, hands-on cyber range labs simulating malware and ransomware events and SOC operations, reinforcing operational decision-making under pressure.
- Assessed student performance through scenario-based evaluations and executive-style deliverables.

Director of Forensics, Incident Response, and Management, LastPass – Remote 08/2022 – 05/2023

Global incident response leader during a period of divesture, organizational transition, and critical security events.

- Led response to high-profile breaches by [redacted] including source code repository compromise and S3 exfiltration of customer data, quickly containing incidents, preventing further loss and strengthening long-term security practices.
- Developed and implemented the newly-divested company's first cybersecurity incident response plan aligned with corporate crisis protocols and involvement from several cross-functional teams.
- Established standardized incident response documentation, escalation plans, and service directories in PagerDuty, Terraform, and GitHub, strengthening security technology integrations with Infrastructure as Code (IaC).
- Delivered high-impact incident reviews to senior leadership, enhancing transparency and confidence in IR Operations.

Manager of Incident Detection and Response, Phreesia – Remote 05/2021 – 08/2022

Built and led a capable detection and response team serving a cloud-native, healthcare-focused technology company.

- Directed detection and incident response for a hybrid infrastructure and SaaS platforms, applying cloud security expertise to reduce response time by 20% and minimize security incidents through improved processes.
- Designed and led monthly tabletop exercises across business units to strengthen readiness and communications.
- Reduced incident response times and audit findings for HITRUST, PCI, and SOC2 by 40% through effective security incident management and process improvements.

Senior Cybersecurity Engineer (contract via TekSystems), T-Mobile – Bellevue, WA 10/2019 – 04/2021

Drove cybersecurity initiatives during the T-Mobile/Sprint merger within the Digital Services Organization

- Designed IAM and integration strategies post-merger, eliminating access issues and ensuring secure, uninterrupted operations for over 5,000 users across both companies.
- Performed threat modeling across the hybrid infrastructure using the STRIDE methodology, applying risk management principles to achieve a 25% reduction in security incidents and prevent potential breaches.
- Mentored junior engineers and guided secure development efforts in cloud and B2B services.

Senior Technical Program Manager, Amazon.com – Seattle, WA 03/2014 – 07/2019

Operational leader within Amazon.com's (E-commerce) Security Incident Response Team (SIRT)

- Implemented a post-compromise mobilization architecture that ensured SIRT operations continued without interruption and reduced business downtime after security incidents.
- Led the deployment of CrowdStrike Falcon across 36 subsidiaries via a walled-console approach.
- Created credential dump de-duplication and management system using Bayesian Analysis and risk-based scoring.
- Proactively uplifted entire SSLv3 e-commerce infrastructure to TLSv1.2 to protect against POODLE vulnerability heading into Black Friday and the 2014 Holiday shopping season. Countermeasures included both server side patching and client/browser fingerprinting messaging to upgrade vulnerable browsers.

EDUCATION

- **PhD(c), Organizational Management / IT Management**, Capella University – Minneapolis, MN
- **MBA, Information Technology Management**, Keller Graduate School of Management – Charlotte, NC
- **MISM, Information Security Management**, Keller Graduate School of Management – Charlotte, NC
- **BS, Computer Science**, College Misericordia – Dallas, PA
- **BAT, Cybersecurity,** Collin College – McKinney, TX (in progress)
- **Leadership Certificate**: Extreme Ownership Academy, Echelon Front – Virtual (in progress)

CERTIFICATIONS

- **Security Blue Team, Level 1**
- **SANS GCIH (expired)**
- **AWS Certified Cloud Practitioner**
- **Qualys QualysGuard Certified Professional**
- **ISACA CISM (expired)**
- **EC-Council Certified Ethical Hacker**
- **ISC(2) CISSP**