# KENNETH YERRID

Melissa, TX | (704) 231-2400 | kcyerrid@proton.me
linkedin.com/in/kcyerrid | kcyerrid.com | github.com/kcyerrid

## PROFESSIONAL SUMMARY

Twenty-eight years of cybersecurity leadership. Millions of online shoppers protected. Thousands of vulnerable servers remediated. One consistent thread: building security programs that are resilient, scalable, and business-ready. As a Senior Security Manager with deep roots in SOC operations, incident response, threat intelligence, and GRC, I've operated across some of the most demanding regulated industries — banking, investments, healthcare, and retail. I've taken SOCs from reactive to proactive, integrated MSSP partnerships that extend team capacity, and built cultures where security is a strategic advantage, not just a cost center. CISSP and CEH certified. Ready to lead at the Director level.

## CORE COMPETENCIES

| | | |
|---|---|---|
| Security Operations & SOC Leadership | Incident Response & Management | Threat Intelligence Operations |
| GRC & Risk Management | MSSP Partnership & Integration | Vulnerability Management |
| SIEM Engineering & Operations | Cloud Security (AWS & Azure) | Digital Forensics & Malware Analysis |
| MITRE ATT&CK & Threat Modeling | Reg. Compliance (HIPAA, PCI-DSS, SOC 2, ISO 27001, HITRUST) | Team Building & Servant Leadership |

### Tools & Platforms

| | | |
|---|---|---|
| Microsoft Sentinel / Defender / Purview | Splunk | CrowdStrike |
| Palo Alto Cortex | Recorded Future | Anomali ThreatStream |
| Filigran OpenCTI | Cyware Intel Exchange | Qualys / Nessus / Nucleus |
| Wiz | ServiceNow / Jira | Kali Linux / SIFT / FLARE |
| Zscaler | | |

## PROFESSIONAL EXPERIENCE

### Information Security Operations Manager

09/2023 – Present

*loanDepot*

*Melissa, TX*

- Inherited an undocumented, ad hoc Level 1 SOC and systematically matured the program by upskilling five analysts to Senior-level Tier 2 operators, integrating BlueVoyant as MSSP for Tier 1 coverage, and migrating the SIEM/SOAR from Palo Alto Cortex to Microsoft Sentinel — reducing MTTD by 78% and driving on-target SLA performance to 98%.
- Served as a key security leader during the high-visibility January 2024 breach, providing operational direction and coordinating response efforts across the organization to contain impact and accelerate recovery.

- Expanded the security technology ecosystem by deploying and integrating CrowdStrike Falcon Complete (Endpoint, Identity Protection, CSPM, and Counter Adversary Operations), Zscaler, Abnormal, Wiz, and Nucleus — establishing comprehensive visibility across endpoint, identity, cloud, and network attack surfaces.

### Director of Forensics, Incident Response & Management

08/2022 – 05/2023

*LastPass*

*Remote*

- As one of the first two security leaders at the newly independent LastPass, led the organization's response to two simultaneous high-visibility breaches involving source code exfiltration and the theft of encrypted password vault backups from AWS S3 — coordinating forensic investigation, containment, and executive communications under intense public and regulatory scrutiny.
- Built the Incident Management function from the ground up, delivering LastPass' enterprise cybersecurity incident response plan, hiring and developing four incident captains, and establishing Security Operations and IR capabilities for a nascent organization mid-crisis.
- Architected and executed a greenfield infrastructure migration — including OpsGenie to PagerDuty transition — leveraging Infrastructure as Code via Terraform and GitHub to establish a scalable, repeatable operational foundation for the new organization.

### Manager of Incident Detection & Response

05/2021 – 08/2022

*Phreesia*

*Remote*

- Inherited an ad hoc, undocumented security operations function and drove the organization to CMM Level 2 maturity across incident response and detection engineering — hiring four staff (2 analysts, 2 engineers), authoring a formal IR policy, and establishing procedures, runbooks, and monthly cross-functional tabletop exercises that reduced MTTD by 40% and MTTR by 63%.
- Championed and built a net-new Detection Engineering program from inception to CMM Level 1.5, establishing a structured, repeatable approach to threat detection that meaningfully elevated the organization's ability to identify and respond to emerging threats.
- Partnered closely with the Information Security Governance team to achieve SOC 2 certification, navigate the PCI ROC process, and position the organization for HITRUST certification — delivering a compliance posture commensurate with Phreesia's obligations as a healthcare SaaS provider.

### Senior Cybersecurity Engineer

10/2019 – 04/2021

*TekSystems (placed at T-Mobile)*

*Remote*

- Served as a senior security advisor to T-Mobile business units, managing multiple concurrent projects and applying STRIDE threat modeling to identify vulnerabilities early in the development lifecycle — enabling teams to shift left on remediation and deliver solutions on-time and within budget.
- Designed and led Identity and Access Management integration strategies following the T-Mobile/Sprint merger, ensuring seamless and secure access to both infrastructures for 5,000 employees across the combined organization.
- Partnered cross-functionally with development and product teams to embed security best practices into solution delivery — translating complex security requirements into actionable guidance that balanced risk reduction with business velocity.

### Senior Technical Program Manager

03/2014 – 07/2019

*Amazon.com*

*Seattle, WA*

- Served as the single point of contact for all security programs impacting Amazon Retail's SOC and Incident Response teams, delivering 40+ projects ranging from $25K to $40M in budget — including the emergency remediation of thousands of externally-facing web servers from the POODLE vulnerability ahead of the 2014 holiday season, protecting millions of online shoppers.
- Orchestrated the enterprise-wide deployment of CrowdStrike across 250,000 instances spanning 36 subsidiaries — each with its own independent management plane — establishing unified endpoint visibility at massive scale across a complex, distributed organization.
- Engineered an intelligence pipeline to ingest, correlate, deduplicate, and risk-score external credential dumps using Bayesian analysis, delivering actionable threat intelligence to the SOC and significantly improving the organization's ability to proactively respond to account compromise threats.

### Adjunct Instructor

10/2020 – 02/2025

*IronCircle / ThriveDX / HackerU*

*Remote (Concurrent)*

- Delivered continuing education instruction in Cloud Security, Digital Forensics & Incident Response, Python, and Game Theory to cohorts across California State Fullerton, University of Michigan, and University of Miami — bringing real-world practitioner experience to contextualize course material and accelerate student comprehension.

## EDUCATION

| | |
|---|---|
| **Doctoral Candidate, Organizational Management (ABD)**<br>*Capella University* | In Progress |
| **MBA, Information Security Concentration**<br>*Keller Graduate School of Management* | 2008 |
| **MS, Information Technology Management, Information Security Concentration**<br>*Keller Graduate School of Management* | 2007 |
| **BS, Computer Science**<br>*Misericordia University* | 1997 |
| **Bachelor of Applied Technology (In Progress, Anticipated 2031)**<br>*Collin College* | 2031 |

## CERTIFICATIONS

| | |
|---|---|
| Certified Information Systems Security Professional (CISSP) | **Active** |
| Certified Ethical Hacker (CEH) | **Active** |
| Blue Team Labs One (BTL1) | **Active** |
| AWS Certified Cloud Practitioner | **Active** |
| *Certified Information Security Manager (CISM)* | Expired |
| *GIAC Certified Incident Handler (GCIH)* | Expired |

## PROFESSIONAL AFFILIATIONS

- ISC$^2$ | Member
- Information Systems Security Association (ISSA) — North Texas Chapter | Member
- SANS Community | Member
- Dallas Hacks Association | Member

## PUBLICATIONS & SPEAKING ENGAGEMENTS

### Publications

- Instant Netcat Starter — Packt Publishing (ISBN 978-1849519960)
- Security blog and research articles — kcyerrid.com

### Conference Speaking

- RSA Conference 2012
- DerbyCon 2
- Multiple BSides Conferences & Local Security Meetups (recurring)

### Podcast Appearances

- Detection Engineering Dispatch — Introduced the SCOUT, CIPHER, and ITIDs project suite

## PROJECTS & DEVELOPMENT

- SCOUT (Security Cyber Operations Unified Tracker) — Obsidian-based security operations knowledge management system serving as the unified superset platform for the full SCOUT/CIPHER/ITIDs product suite
- CIPHER (Cyber Intelligence Playbooks, Hunting, Enrichment & Reporting) — Obsidian-based framework for tracking, managing, and operationalizing Cyber Threat Intelligence
- ITIDs (Incident Type Identification Digits) — Original 4-tier incident taxonomy enabling greater consistency and flexibility in SOC incident classification and response
- Homelab Tutorials — Modular, à la carte instructional platform enabling IT professionals to build customized home lab environments
- Backdoors & Breaches Facilitator's Guide — In-progress facilitator's companion for the popular incident response card game