

TIM CARREIRA

INSIDER RISK INVESTIGATIONS • DIGITAL FORENSICS • AI-AUGMENTED DFIR

Springfield, MA | 860-778-7966 | timothycarreira@gmail.com

linkedin.com/in/calltim | github.com/Scubber | thederpweb.com | intel.thederpweb.com

SUMMARY

Insider risk investigator and program builder with nearly two decades in enterprise technology, including seven years in security operations and investigations at global financial institutions. **100+ insider threat, DFIR, and fraud investigations** spanning data exfiltration, data misuse, privacy violations, and policy abuse; investigative interviews conducted alongside HR and Legal since 2022. Currently standing up Voya Financial's enterprise insider threat program: detection engineering across DLP, UEBA, and SIEM; triage and investigative workflow; and governance, while modernizing casework with **Claude, Claude Code, and self-hosted LLMs**. Creator of **insider-intel**, a live OSINT platform that maps insider threat cases from federal court records to the Insider Threat Matrix. CISSP, CCSP, four GIAC DFIR certifications, PMP.

CORE CAPABILITIES

INVESTIGATIONS: Insider risk & corporate investigations • Investigative interviews • Digital forensics (host, network, memory, cloud) • eDiscovery • Evidence handling & case documentation • Threat hunting • Rapid-response assessments

DETECTION & MONITORING: DLP (Proofpoint) • UEBA • SIEM (Splunk — SPL, KQL) • SOAR • EDR/XDR (CrowdStrike) • Detection engineering • Behavioral analytics

OSINT: Open-source research • Court-record mining (PACER, RECAP, CourtListener) • Social & community monitoring • Insider Threat Matrix (ITM) • MITRE ATT&CK

AI & AUTOMATION: Claude & Claude Code • LLM-assisted triage, evidence analysis & reporting • AI agent orchestration • Self-hosted LLMs (Ollama on NVIDIA DGX Spark) • Prompt engineering

CLOUD & PLATFORMS: AWS • Azure • GCP • OCI • CSPM • IAM • Windows • Linux | Python • PowerShell • SQL

FRAMEWORKS & COMPLIANCE: MITRE ATT&CK • NIST 800-53 • NICE • ITAR

EXPERIENCE

Insider Threat Management • IT Security Consultant

Apr 2026 – Present

Voya Financial • Windsor, CT

- Returned to Voya to build the enterprise insider threat program as its senior individual contributor: strategy, governance, detection engineering, and investigative workflows across DLP, UEBA, and SIEM.
- Run insider risk investigations from triage of behavioral detections through forensic collection and analysis, investigative interviews in partnership with HR and Legal, and case reporting to executives.
- Engineer AI-assisted DFIR workflows using **Claude and self-hosted LLMs** to speed up triage enrichment, evidence summarization, and report drafting while keeping sensitive case data in-house.
- Lead proactive insider threat hunts across enterprise data sources to catch data exfiltration and misuse early; develop new risk indicators with Privacy, HR, Legal, and Fraud partners.

Cloud Security Engineer • VP, Cybersecurity

Aug 2025 – Mar 2026

State Street Corporation • Boston, MA

- Led development of a multi-cloud (AWS, Azure, OCI) CSPM capability within Cloud Application & System Security Engineering; matured incident detection & response automations with Wiz Defend and Wiz Cloud.
- Drove remediation of MRAs and other regulatory findings.

Cloud Security Operations Manager • VP, Cybersecurity

Aug 2024 – Aug 2025

State Street Corporation • Boston, MA

- Built and led the Cloud Security Operations program: strategy, governance, and purple-team exercises that matured cloud incident response against a two-year capability roadmap.
- Reported exercise metrics and written assessments to senior stakeholders; partnered with Privacy, HR, and Legal on sensitive investigations.

Senior Cloud Incident Response Analyst · VP, Cybersecurity

Jan 2024 – Aug 2024

State Street Corporation · Boston, MA

- Cloud IR Lead in the Global Cyber Defense Center: rapid containment, triage, and event reporting across AWS, Azure, and OCI.

Threat Hunting & Incident Response · Team Leader

Apr 2023 – Jan 2024

Voya Financial · Windsor, CT

- Directed insider threat investigations, advanced hunts, and forensics involving fraud, data exfiltration, and privacy incidents; conducted investigative interviews and briefed outcomes to business stakeholders.
- Designed and ran enterprise tabletop exercises covering ransomware, insider threat, DLP, and cloud IAM; mentored a global analyst team.
- Architected and maintained a cloud-based DFIR lab for digital forensics, malware analysis, and casework.

Digital Forensics & Incident Response Lead · IT Security Consultant

Mar 2022 – Apr 2023

Voya Financial · Windsor, CT

- Incident commander for critical cybersecurity response; delivered quick-turnaround security assessments for time-sensitive business matters.
- Built advanced Splunk detections and dashboards for behavioral anomalies and insider threat TTPs across multiple application log sources.
- Investigated and contained insider cases involving data misuse, fraud, and privacy violations; partnered with HR and Legal on interviews and produced executive summaries for stakeholders and third-party regulators.

Senior IT Security Specialist · Digital Forensics & Incident Response

Aug 2019 – Mar 2022

Voya Financial · Windsor, CT

- Triageed and contained a high-volume caseload across DLP, privacy, malware, phishing, and data-handling violations.
- Automated SIEM root-cause analysis and EDR response actions with behavioral analytics; communicated findings to business leadership through concise reports and post-incident reviews.

IT Manager — IT Infrastructure & Security

May 2014 – Aug 2019

Engineering Industries eXcellence / Design Automation Associates · Windsor Locks, CT

- Sole IT and security owner for a 50-person ITAR defense-aerospace engineering firm across three offices — multi-site networks, Windows/Linux servers, endpoints, and NIST-aligned security.
- Earlier stint with the firm as an IT Support Specialist (Jan 2009 – Jan 2011).

SELECTED PROJECTS

insider-intel · OSINT platform for insider risk

intel.thederpweb.com

- Built and operate a live intelligence pipeline that mines federal court records (CourtListener/RECAP, targeted PACER) plus curated news and community feeds for real insider threat cases — theft, leaks, and sabotage.
- LLM-assisted extraction maps each filing to Insider Threat Matrix™ techniques, with confidence scoring, an evidence ledger separating definitive artifacts from inferred leads, and hunt reports with ready-to-run SIEM, email, and chat queries.
- Designed and built entirely with **Claude Code**.

AI Investigations Lab · personal research environment

- Self-hosted LLM lab (Ollama on **NVIDIA DGX Spark**) for investigative AI experiments that keep data local; Google **GEAR** (Gemini Enterprise Agent Ready) program participant, building and evaluating AI agents for security workflows.

CERTIFICATIONS

CISSP · Certified Information Systems Security Professional

CCSP · Certified Cloud Security Professional

CCSK v5

GIAC · GCIH (Incident Handler) · GCFA (Forensic Analyst) · GCFE (Forensic Examiner) · GNFA (Network Forensic Analyst)

PMP · Project Management Professional

Verify: credly.com/users/timothy-carreira

EDUCATION & TRAINING

SANS Technology Institute — Graduate Certificate, Incident Response

2019 – 2023

Central Connecticut State University — B.S., Management Information Systems

2015 – 2017

ADVANCED TRAINING: AWS Security – Specialty · AWS Security Engineering · GIAC GCFR (Cloud Forensics) · GIAC GREM (Malware Analysis)

COMMUNITY: FS-ISAC — member; preparing summit talk on building insider threat programs · InfraGard · Cloud Security Alliance