Robert Higham

Dallas-Fort Worth, TX • LinkedIn

Professional Summary

Results-driven cybersecurity leader with 20+ years of success in building security architectures and delivering cybersecurity products and services across diverse industries. Experience leading global teams of highly skilled security researchers and engineers and building cybersecurity programs. Seeking a senior leadership role to build and mature cybersecurity teams/programs, flexible on location. Excels in team leadership, governance, and embedding security into operations. Proficient in policy, architecture, and vendor risk, with a passion for evolving threat defense.

Certifications: GIAC-CFA, CISSP, CRISC, OSCP, FAIR, MS Azure Security Engineer Associate

---

Skills Summary

- Skilled in communicating technical roadmaps and project status to stakeholders at all levels.
- Demonstrated ability to lead and motivate cross-functional, interdisciplinary teams.
- Strong problem-solving skills with the ability to influence decision-making through effective negotiation.
- Ability and willingness to perform hands-on, engineering and operational work as needed.
- Proficient in managing robust data pipelines using Apache technologies (e.g. Spark, Kafka and Flink).
- Strong command of Python libraries (e.g., Pandas, NumPy, Scikit-learn) for data manipulation, analysis, and engineering tasks.
- Proven experience in managing end-to-end 3rd party data ingestion and integration from diverse sources, including network, cloud, application, and endpoint security platforms.
- Demonstrated ability to leverage generative AI to create agentic and advanced RAG solutions.

Professional Experience

Director, Counter Threat Unit - Detection Research | SecureWorks, Inc. | September 2023 – Present

- Directed a global Security Operations team, managing security for 1,000+ clients and processing over 700 billion cloud, endpoint and network security events daily.
- Reduced missed detections crit-sits from ~2% to 0.4% (exceeding 1% target), improving customer satisfaction through escalation redesign and engineering collaboration.
- Drove 80% reduction in ticket turnaround times by optimizing detection engineering workflow with emerging threat intelligence and AI-powered technologies (machine learning, generative AI).
- Facilitated strategic planning, performance reviews and budget for a multi-million dollar department.

Senior Researcher | SecureWorks, Inc. | November 2019 – September 2023

- Led the company-wide effort to prepare for and participate in the 2023 MITRE ATT&CK evaluation.
- Developed a Threat-Hunting-as-a-Service offering that surpassed revenue targets by 500%.
- Created and delivered a threat hunting skill development workshop to over 150 internal analysts.

- Strategically developed and delivered a customer facing threat hunting workshop, redirecting over $1 million in expiring Incident Management Retainer (IMR) credits to my department to fund research.
- Co-developed a Python-based threat hunting tool which achieved 500+ FTE hours per month savings.
- Delivered 20+ public speaking engagements at conferences, chapter meetings, and CISO roundtables.

Product Manager - Security Operations | State Farm Insurance | July 2014 – November 2019

- Guided the formation and recruitment of the Security Analytics and Cyber Threat Intelligence teams.
- Led a 6-person team of data and security analysts in threat hunting and security analytics, enhancing SOC operations through intelligence-driven security monitoring.
- Streamlined threat hunting and detection engineering workflows by implementing Agile principles.
- Reduced average cyber threat intelligence triage and action times from days to hours by developing and deploying an efficient workflow and prioritization matrix.
- Led incident response planning, tiger team activities and tabletop exercises.

Senior Analyst - Business Application Security | State Farm Insurance | May 2007 – July 2014

- Spearheaded the development of the Information Security Risk Management program for the company, creating and delivering training programs and technical documentation for 30+ risk professionals.
- Developed and oversaw enterprise information security policies, standards, guidelines, and the Secure Development Lifecycle (SDL) and risk exception processes, providing guidance to the CISO and Senior Counsel on risk acceptance decisions.
- Facilitated multiple (20+) risk assessments, evaluating security controls for third-party vendors and internal tool development projects.
- Led multiple internal audits and compliance assessments across PCI, ISO 27001, HIPAA, and NIST.

Education

- **M.S. Cybersecurity** | *University of South Florida, June 2017* – Focus: Cyber Threat Intelligence
- **B.S. Information Technology** | *Franklin University, January 2007* – Graduated Cum Laude*
- **Technology Leadership Certificate** | eCornell, February 2025 - *In Progress*

Professional Engagement & Community Involvement

- Previous mentor in **AFA CyberPatriot Competition** (*2 years*).
- Actively volunteer through Salkehatchie Summer Service where I mentor and teach young adults
- Participate in **Capture the Flag (CTF) competitions** to refine skills.
- Regularly contribute insights and research in **cybersecurity networking, blogging, and social media**
