Thomas J. Fosbenner, Jr.

Security Operations Executive | SOC Transformation | MDR/MSSP | AI-Enabled Analyst Acceleration

Dayton, OH | Open to travel and relocation | (480) 387-8900 | dotcomdewd@me.com | linkedin.com/in/tfosbenner

PROFESSIONAL SUMMARY

Security operations and cybersecurity executive with 20+ years of experience leading SOC, incident response, security engineering, infrastructure, GRC, cloud, and IT operations across MSSP/MDR, SaaS, healthcare, manufacturing, fintech, gaming, and e-commerce environments. Strong record of improving operational maturity, reducing alert noise, building teams, maturing processes, supporting 24x7 operations, and helping organizations deliver measurable improvements in detection, response, compliance, and service quality.

Currently focused on AI-enabled SOC transformation, including agent workflows, LLM-assisted documentation, analyst decision support, false-positive reduction, process automation, and practical use of ChatGPT, Grok, Claude Code, and private Ollama environments for security operations use cases.

OPERATIONAL IMPACT HIGHLIGHTS

- Reduced SOC alert volume by 20% within 60 days at NuHarbor by tuning false positives and improving alert quality.
- Support a 24x7 SOC serving state and government entities as well as large enterprise clients.
- Built security programs from the ground up at Dutchie and Blink Health, including SOC, incident response, engineering, GRC, audit readiness, and executive reporting.
- Led Splunk Cloud and MSSP/MDR transition at Aristocrat while identifying $500K+ in annual savings through tool rationalization.
- Built and led distributed technical teams of up to 30 and oversaw 60+ security applications across 130,000+ systems at eBay/PayPal.

CORE SKILLS & KEYWORDS

Leadership: CISO Advisory, Security Program Development, Cybersecurity Strategy, Executive Reporting, Board Reporting, Security Roadmaps, Security Transformation, Team Building, Budgeting, Vendor Management

Security Operations: SOC Leadership, 24x7 Security Operations, Incident Response, Alert Triage, Threat Detection, MDR/MSSP Oversight, False Positive Reduction, Vulnerability Management, Detection Improvement

GRC & Compliance: SOC 1, SOC 2, HIPAA, HITRUST, PCI, NIST, ISO 27001, Policy Development, Risk Management, Audit Readiness, Control Maturity

AI & Automation: AI Security Operations, Agentic AI, AI Agents, ChatGPT, Grok, Claude Code, Ollama, LLM Evaluation, Security Automation, Workflow Automation, Documentation Automation

Technical: Linux, AWS, Azure, Splunk, SIEM, EDR, DLP, CASB, Tenable, Microsoft Security Tools, Docker, Raspberry Pi, Infrastructure Security, Cloud Security

IT Operations: Global IT Operations, Manufacturing IT, Endpoint Management, Printers, Procurement, Remote Hands, Logistics Support, Systems Administration, Infrastructure Operations

PROFESSIONAL EXPERIENCE

Security Operations Manager / Cybersecurity Transformation Leader | NuHarbor Security | Remote | 12/2025 - Present

- Work directly with the CEO, Executive Vice President, and senior leadership to improve security operations maturity, reshape service delivery, and strengthen organizational execution across a 38-employee cybersecurity services company.
- Support a 24x7 Security Operations Center serving state and government customers as well as large enterprise clients, with focus on improving analyst efficiency, alert quality, and client delivery outcomes.
- Reduced alert volume by 20% within 60 days by tuning false positives, improving signal quality, and reducing unnecessary analyst workload without weakening monitoring coverage.
- Partner with leadership to review and improve policies, operational procedures, staffing alignment, service offerings, and integration approaches for new states, companies, and business expansion activities.
- Contribute to proposal development and executive proposal reviews, helping align customer commitments, service delivery capabilities, staffing models, and operational realities.
- Lead AI enablement efforts for security operations, evaluating how AI agents, workflow automation, analyst decision support, documentation, and process automation can accelerate threat detection, triage, and response.
- Build security tools, documentation, and operational processes using ChatGPT, Grok, Claude Code, and a private Ollama server to deepen hands-on LLM experience and test practical AI use cases for cybersecurity operations.

Director of IT Operations & Security | United Wheels / Huffy | Remote / Global | 09/2024 - 12/2025

- Owned global IT operations and cybersecurity for a manufacturing organization, leading security strategy, IT execution, vendor management, purchasing, budgeting, hiring, infrastructure support, and global operational support.
- Led approximately 10 team members and coordinated global remote-hands support across corporate, manufacturing, logistics, and international operations.
- Managed business-critical IT services including systems, endpoints, printers, infrastructure, support processes, procurement, vendor negotiations, and technology roadmap execution.
- Supported manufacturing security and operational risk needs involving production environments, shipping/logistics, containers, international travel, cross-border business activity, and distributed workforce support.
- Introduced AI-driven opportunities to support finance, bookkeeping, purchasing, and operational efficiency use cases across business functions.
- Assessed infrastructure, security controls, team capabilities, vendor relationships, and operational gaps to build a practical roadmap for improving IT and security maturity.

Head of Information Security, IT & Acting CISO | Dutchie | Remote | 05/2021 - 01/2024

- Hired as the first security leader to build the information security program from the ground up for a rapidly scaling SaaS company supporting more than 7,400 customer locations.
- Built and led an approximately 11-person global security organization covering Security Operations, Security Engineering, Security GRC, Application Security, and Incident Response.
- Advanced the company from little/no formal security program to a mature, audit-ready security function, achieving SOC 1, SOC 2, and HIPAA baseline readiness/certification within approximately 18 months.
- Developed and executed cybersecurity roadmaps, policies, procedures, risk management processes, security awareness, incident response practices, and executive reporting cadences.

Director, Global Information Security | Aristocrat Technologies | Austin, TX | 05/2020 - 03/2021

- Directed global security teams across Attack Surface Management, Security Engineering, and Security Operations, reporting directly to the CISO.
- Identified more than $500K in annual savings through application and security tool rationalization while improving operational efficiency.
- Led the strategic transition to Splunk Cloud and selected a new MSSP/MDR partner for Tier 1 SOC operations.
- Drove large-scale global initiatives including DLP, CASB, Splunk, and cross-business security improvement programs.

Director, Security Operations, Engineering & Infrastructure | Blink Health | Boston, MA | 12/2018 - 05/2020

- Built a security program from the ground up, including incident response, data monitoring, SOC development, staffing, security engineering, and security operations practices.
- Supported HIPAA, PCI, and HITRUST audit readiness and certification activities while reporting security posture, incidents, and threats to C-level executives.
- Implemented foundational security technologies including SIEM, EDR, endpoint protection, and cloud/on-premises security tooling across AWS and enterprise environments.
- Collaborated across business units to improve disaster recovery planning, incident communication, and enterprise security maturity.

Senior Manager, Commerce Operations | Sony Interactive Entertainment (PlayStation) | San Diego, CA | 08/2017 - 12/2018

- Led global commerce platform operations and managed a team of subject matter experts supporting PlayStation's worldwide commerce stack.
- Hired and managed a team of 10+ resources, including overseas support, to support AWS migration and global platform operations.

Manager, Information Security Engineering, Delivery & Tools | eBay / PayPal | Scottsdale, AZ | 07/2010 - 04/2017

- Built and led a distributed team of approximately 30 engineers and information security specialists across the United States and Israel, responsible for managing 90% of PayPal's information security infrastructure.
- Oversaw 60+ business-critical InfoSec applications across more than 130,000 Red Hat, Ubuntu, and Windows systems.

Earlier Experience: Turner Broadcasting Systems - Senior Systems Engineer, e-commerce; The Weather Channel - Senior Systems Administrator, Production Environment.