MELISSA BISCHOPING

melissa@securitysphynx.com | linkedin.com/in/mbischoping | securitysphynx.com

EXECUTIVE SUMMARY

Cybersecurity executive with 10+ years progressive technology experience, currently leading secure operations and threat detection enablement for a global industrial software portfolio as a direct report to the CISO. Track record building security capabilities from charter to operational scale across both enterprise and product security environments: reducing mean time to detect, respond, and contain (MTTD/MTTR), rationalizing fragmented tool stacks, and leading cross-functional teams in complex global matrixed organizations. Deep expertise in security operations strategy, detection engineering, security tooling evaluation and consolidation (SOAR, SIEM, EDR/XDR, CNAPP, MDR), vulnerability intelligence, security metrics and executive reporting, AI security, and automation of investigation and response workflows. SANS Technology Institute Board Member and SANS Instructor Candidate (LDR514) recognized for driving measurable security outcomes through data-driven leadership.

PROFESSIONAL EXPERIENCE

Siemens Digital Industries Software | Washington DC-Baltimore Area

Director, Secure Operations & Enablement | *June 2026 - Present*

- Recruited to lead threat detection enablement and automation strategy for a global industrial software portfolio, reporting directly to the CISO. Chartered to compress the interval between incident onset and containment, and to build the measurement system that proves it.
- Established the security measurement and executive reporting program as primary charter deliverable: defined time-to-detect, respond, contain, and recover targets alongside automation ROI and adoption metrics, replacing a manual monthly reporting cycle consuming a week of analyst effort per month.
- Leading evaluation and consolidation of the security operations technology stack across cloud workload protection, managed detection and response, and log management, converting overlapping point solutions into a rationalized platform strategy under enterprise-wide contract alignment.
- Sponsoring asset inventory and configuration management reconciliation as the foundation for detection coverage, resolving inventory discrepancies across endpoint, cloud, and CMDB data sources that gate the majority of downstream security operations work.
- Building the Secure Operations & Enablement organization and applying AI-assisted and agentic workflows to automate investigation, tool integration, and reporting functions across cyber defense, DevOps, SRE, and product engineering in a global matrixed environment.

Tanium | Washington DC-Baltimore Area

Sr. Director, Security & Product Design Research | *September 2024 – June 2026*

Director, Endpoint Security Research | *October 2021 – September 2024*

Technical Account Manager, Commercial US | *March 2021 – October 2021*

Enterprise Services Engineer, Tanium Federal (DOD/DHS) | *June 2020 – March 2021*

- Built Security & Product Design Research organization from the ground up: authored charter, recruited 3 Directors, and led 8 direct/matrixed contributors across 7 cross-functional organizations in a global matrixed environment. Influenced $1.3M+ in strategic cybersecurity investment and tooling decisions.
- Scaled threat detection and response capability (Tanium Guardian) from manual process to automated delivery, reducing mean time to release from 5-7 days to 12 hours during critical industry events. Built automated pipeline leveraging CVE/NVD, CVSS, and EPSS prioritization with a dedicated 3-person team.

- Designed and implemented telemetry-driven analytics program to identify security tooling gaps and prioritize detection investments against actual customer threat landscape. Shifted organization-wide security operations prioritization from reactive to data-driven, enabling continuous gap analysis of the technology stack.
- Led threat detection and vulnerability research to identify emerging risks, evaluate security tooling efficacy, and close detection gaps in partnership with Product and Engineering. Original research (LOLRMM) led to discovery of previously unreported adversary tooling and drove detection engineering improvements.
- Conducted continuous gap analysis of security operations technology stack, evaluating and recommending tooling improvements across endpoint detection, cloud security, and network monitoring. Delivered technology radar assessments to engineering leadership for stack modernization decisions.
- Single technical authority for incident response executive messaging during major security events; delivered after-action reviews, root cause analysis, and containment recommendations to CEO, CTO, and SVP Engineering under 24-hour SLA.
- Led AI security strategy research including analysis of emerging AI threats (agentic AI exploitation, open weight model risks), producing executive-level risk assessments and defensive automation frameworks. Pioneered use of AI-assisted workflows to accelerate security operations and investigation functions.
- Developed and operationalized security guardrails framework for SaaS product onboarding, converting manual compliance checklists into automated security checks. Drove attack surface reduction through lifecycle management, patch coordination, and hardening standards across the product portfolio.
- Primary point of contact for public-private intelligence-sharing partnerships. Managed 10-12 pre-disclosure vulnerability intelligence items monthly under 24-hour SLA.
- Represented organization as trusted industry voice through 10+ annual publications (Dark Reading, CyberScoop, SecurityWeek), monthly global conference speaking (US/EMEA/AU/APAC), and executive briefings for customer CISOs/CIOs.

Calumet Specialty Products Partners, L.P. | Shreveport, Louisiana

Cyber Security Engineer | *June 2019 – June 2020*

I.T. Administrator | *June 2018 – June 2019*

- Built comprehensive security operations program for 2,000-employee enterprise across 18 locations. Led end-to-end SOC implementation including vendor selection, sensor deployment, SIEM policy tuning, network monitoring configuration, and incident response process development.
- Improved critical systems compliance from 65% to 92% in three months through vulnerability management automation, SCCM remediation, and cross-team patch management coordination. Established lifecycle management practices for attack surface reduction across multi-site infrastructure.

EDUCATION

SANS Technology Institute | M.S. Information Security Engineering, 2024 (GPA 3.91, RSA Security Scholar)

Colorado State University | B.S. Information Technology, 2018 (Summa Cum Laude)

University of Wyoming | B.S. Psychology, 2015

INDUSTRY LEADERSHIP & CREDIBILITY

- SANS Technology Institute Board of Directors | Board Member (2026 – Present)
- SANS Instructor Candidate | LDR514: Strategic Planning, Policy & Leadership
- Consistent media presence: 10+ articles annually across major cybersecurity publications (2022-present)
- Rapid-response expert commentary: quoted within 24 hours of major security incidents

- Talks/Videos: securitysphynx.io/videos | Media: securitysphynx.io/news

CERTIFICATIONS & CLEARANCE

12 Active GIAC Certifications (Co-termed through September 2028) | securitysphynx.io/certs

Strategic & Leadership: GIAC Strategic Planning, Policy & Leadership (GSTRT) | GIAC Certified Project Manager (GCPM) | GIAC Security Professional (GSP)

Threat Intelligence & Operations: GIAC Cyber Threat Intelligence (GCTI) | GIAC Certified Incident Handler (GCIH) | GIAC Certified Intrusion Analyst (GCIA) | GIAC Defensible Security Architecture (GDSA)

Forensics & Analysis: GIAC Experienced Forensic Expert (GX-FE) | GIAC Experienced Forensic Analyst (GX-FA) | GIAC Certified Forensic Analyst (GCFA) | GIAC Certified Forensic Examiner (GCFE) | GIAC Security Essentials (GSEC)

In Progress: Project Management Professional (PMP)

Security Clearance: U.S. Secret (Issued 2020, Active)

Published by Melissa Bischoping at securitysphynx.com/resume for direct inquiries. Not authorized for submission, representation or resale by recruiters, staffing agencies or third parties without written consent. melissa@securitysphynx.com