PHILLIP TARRANT

Morrison, TN • (706) 294-6733 • ptarrant@gmail.com • LinkedIn: linkedin.com/in/phillip-tarrant-cyber

HEAD OF SECURITY OPERATIONS CENTER | MSSP OPERATIONS EXECUTIVE

Strategic and hands-on Security Operations leader with 20+ years of cyber experience and a proven record of transforming SOC performance in commercial MSSP environments. Scaled SOC operations from 16 to 52 clients while expanding service offerings, strengthening quality, and establishing repeatable operational structure. Responsible for vendor rationalization and pricing realignment that increased SOC profitability from 18% to 52% (including an 80% peak quarter) and contributed to 15% year-over-year net income growth. Expert in SIEM, SOAR, DFIR, threat detection, automation, and high-performing team leadership.

Senior Information Security Consultant — Confidential (2025–Present)

• Engaged as interim SOC Director for multiple MSSPs, restructuring workflows, staffing models, and service delivery.

• Led SOC modernization initiatives including process redesign, automation adoption, and cross-tenant security governance.

• Oversaw global SOC operations for a major U.S. Defense Space sector supplier across multi-tenant Microsoft environments.

• Directed enterprise-scale Vulnerability Management Program (Qualys) for a top U.S. fintech organization.

• Advised executive leadership on pricing strategy, risk posture, compliance frameworks, and operational performance.

Director of Automation — Compuquip Cybersecurity (2024)

• Built enterprise automation platform processing 3,500+ tickets weekly with 47% fully automated resolution.

• Developed next-generation SOAR and AI-assisted workflow architecture using Python, AWS Lambda, and custom LLM pipelines.

• Drove automation roadmap aligning SOC efficiency gains with MSSP service scalability and cost reduction.

• Mentored engineering team on automation engineering, decision-logic development, and AI-assisted enrichment.

SOC Director — Compuquip Cybersecurity (2023–2024)

• Scaled SOC from 16 to 52 clients across multiple verticals while expanding MDR, DFIR, and proactive services.

• Increased SOC profitability from 18% to 52% via vendor consolidation, pricing restructuring, and workflow optimization.

• Led 17-person cross-functional team including SOC, Red Team, and remediation engineering resources.

• Oversaw DFIR engagements, offensive security operations, vulnerability scanning, patching, and MDR programs.

• Produced executive-level reporting, APT situational awareness briefs, and quarterly operational KPIs.

• Partnered with C-suite leadership on MSSP strategy, client retention, and long-term service planning.

SOC Technical Manager — Compuquip Cybersecurity (2021–2023)

• Built foundational SOC SOPs, workflows, and training curriculum for a rapidly scaling MSSP.

• Led incident research, detection development, and advanced analyst mentorship programs.

• Developed monthly threat landscape reports and SOC performance metrics used for client and board reporting.

• Standardized triage and investigation processes across SOC shifts to improve consistency and quality.

Sr. Cyber Security Architect — TST (2020–2021)

• Directed cloud security architecture, compliance programs, and phishing/developer training initiatives.

• Designed automated attack simulation and detection validation tooling.

• Guided organization through PCI and NIST 800-series audits while strengthening overall security posture.

• Negotiated vendor contracts delivering substantial annual cost savings.

Senior Cyber Security Engineer — Intercontinental Exchange (2020)

• Designed security data pipeline architecture for large-scale SIEM ingestion and analysis.

• Automated SOC triage and investigation workflows reducing analyst workload and dwell time.

• Developed dashboards supporting threat hunting, vulnerability management, and incident tracking.

Cyber Security Engineer — Intercontinental Exchange (2018–2020)

• Led investigations for multi-host compromises across distributed environments and teams.

• Developed forensic procedures, malware analysis practices, and IR playbooks.

• Trained analysts through custom malware exercises and forensic labs.

Technical Services Manager — NWTF (2015–2018)

• Led IT & security operations for 300+ staff with an 8-person engineering team.

• Managed infrastructure expansion, vendor negotiations, and web/app security.

• Delivered $50K+ yearly savings by replacing outsourced systems with internal solutions.

Education

Associate Degree in Network Administration — Virginia College (4.0 GPA)

Certifications

• GIAC GWAPT — Web Application Penetration Tester

• GIAC GCFA — Forensic Analyst

• GIAC GCIH — Incident Handler

• CompTIA A+