

Phillip Tarrant

Director, Detection Engineering & Threat Hunting | Security Automation & AI Leader

ptarrant@gmail.com • (706) 294-6733

www.linkedin.com/in/phillip-tarrant-cyber • Morrison, TN

Security leader with 20+ years of experience building and leading detection engineering, threat hunting, and SOC operations across MSSP and enterprise environments. Proven director-level track record managing multiple large teams, restructuring SOC workflows, and scaling detection and response programs. Deep technical foundation in digital forensics, malware reversing, incident response, and threat hunting with and without AI integration. Led MSSP operations for 50+ business clients encompassing 150,000+ assets and 1 million+ users. Experienced AI and automation leader with expertise in SOAR engineering, prompt engineering, LLM integration, AI security and guardrails, and deploying AI-driven detection solutions in secure, regulated environments.

Career Experience

Principal Security Engineer TopBuild Corp, Remote *Feb 2026 – Present*

Lead engineer owning security automation, AI development, and SIEM/logging strategy for the enterprise security program; drive detection engineering, threat hunting tooling, and analyst enablement while advising leadership on strategic security investments.

- Own enterprise security automation, AI development, and SIEM/logging strategy across the security program
- Architected and built a custom SOAR web application from the ground up — 20+ automated response actions unifying detection, reporting, and response across Microsoft 365, CrowdStrike, Google SecOps, and ReliaQuest data sources
- Engineered a 'user activity tracker' that accelerates incident triage and proactive threat hunting across enterprise telemetry
- Automated end-to-end quarantine email release across Microsoft 365 and Abnormal, cutting analyst response time on phishing and malicious mail
- Mentor 2 junior engineers on a lean 5-person security team in secure coding and cybersecurity-forward AI usage; advise senior leadership on strategic detection engineering and security investments

Senior Information Security Consultant Confidential, Remote *Dec 2024 – Feb 2026*

Contract consulting role providing cybersecurity leadership and technical expertise.

- Managing SOC operations for US Defense Space market supplier across multiple Microsoft tenants
- Managed Vulnerability Management Program for one of the largest fintech clients in the US using Qualys
- Director role at MSSP restructuring SOC flow and training SOC staff
- Designing secure architectures and providing compliance guidance (HIPAA, PCI-DSS, GDPR, NIST 800-53)

SOC Technical Manager → SOC Director → Director of Automation Compuquip Cybersecurity, Tampa/Doral, Florida *Dec 2020 – Nov 2024*

Progressive leadership roles managing SOC operations, Red Team, AI development, and security automation for MSSP clients.

- Grew SOC client base from 16 to 52 customers; improved profitability from 18% to 52% margin
- Built automation handling 3,500 tickets weekly with 47% closed without human involvement
- Managed team of 17 direct reports across SOC, Red Team, and DFIR engagements

- Oversaw all AI development in a secure MSSP environment, building AI-powered security automation using Python, AWS Lambda, LLMs, and SOAR platforms
- Designed and implemented prompt engineering frameworks and AI guardrails to ensure safe, accurate, and auditable AI outputs in production security workflows
- Built RAG-based knowledge systems and LLM-driven triage pipelines for automated threat classification and analyst augmentation
- Established AI governance policies including model evaluation, output validation, and security controls for LLM deployments

Sr. Cyber Security Architect Travel Syndication Technology (TST), Alpharetta, Georgia *Mar 2020 – Dec 2020*

Responsible for security architecture, training programs, and compliance across the organization.

- Steered organization through PCI and NIST 800 series audits
- Created custom tools to automate attacks against infrastructure and design detections
- Saved \$10,000+ through effective vendor/supplier negotiations

Cyber Security Engineer → Senior Cyber Security Engineer Intercontinental Exchange, Marietta, Georgia *Jul 2018 – Mar 2020*

Incident Response/Digital Forensics lead, promoted to Architecture and Automation Team.

- Lead investigator on critical incidents; managed multi-server compromise investigations across three teams
- Led Malware Analysis in sandboxed environments; mentored junior analysts
- Designed security data flow pipelines and automated SOC triage tools

Technical Services Manager The National Wild Turkey Federation, Edgefield, South Carolina *Sep 2015 – Jul 2018*

Managed IT team supporting 300+ staff members with focus on infrastructure and security.

- Managed team of 8 technicians and developers supporting 300+ staff members
- Migrated 3rd party tools to in-house solutions saving \$50,000+ yearly
- Managed security of entire web presence including network and application code

IT & Systems Administration Roles Earlier Experience *Dec 1998 – Dec 2014*

Progressive IT roles including Network/Server Administrator at NWTF, System Administrator at Morgan Thermal Ceramics, IT Coordinator at Briarwood Academy, and Technical Support at Sitel Group.

Education, Certifications, and Awards

GWAPT - Web Application Penetration Tester, GIAC, 2019

GCFA - Forensic Analyst, GIAC, 2018

GCIH - Incident Handler, GIAC, 2017

Lethal Forensicator Coin Winner, SANS/GIAC, 2018

SANS Challenge Coin for excellence in digital forensics

Associate in Network Administration, Virginia College, 2014 – 2016

GPA: 4.0

Technical Skills

Security Operations, SIEM & SOAR: Splunk, ELK Stack, Microsoft Sentinel/Defender, Google SecOps (Chronicle), CrowdStrike, ReliaQuest, Sentinel One, Rapid7 IDR, Swimlane, D3 SOAR, Torq, Custom SOAR Development, Playbook Development

Threat Detection, DFIR & Red Team: Darktrace, Tanium, Vectra, FireEye, Volatility, Malware Analysis, Incident Response, Detection Engineering, Threat Hunting, Abnormal Security, Metasploit, Purple Team

AI/ML & Automation: AWS Bedrock, LLMs, RAG, Prompt Engineering, AI Security & Guardrails, AI Governance, Agentic AI, Model Evaluation, Python Automation

Cloud, Infrastructure & Programming: AWS, Azure, Oracle Cloud, Windows Server, Linux/UNIX, Active Directory, Docker, Kubernetes, Python, PowerShell, Bash

Compliance & Frameworks: NIST 800-53, PCI-DSS, HIPAA, GDPR, CIS Benchmarks

Leadership & Management: Team Leadership (17+ reports), MSSP Operations, Budget Management, Vendor Negotiations, Training & Mentorship