

Phillip Tarrant

Principal Security Engineer | Security Automation & AI Engineering

ptarrant@gmail.com • (706) 294-6733

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

Principal-level security engineer with 20+ years building detection and AI-driven automation across MSSP and enterprise environments. Ships production tooling end to end — custom SOAR platforms and LLM triage pipelines; built automation that closed 47% of 3,500 weekly tickets with no human touch. Deep DFIR and threat-hunting roots, now focused on applied AI security.

Career Experience

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

Lead engineer owning security automation, AI development, and SIEM/logging strategy for the enterprise security program; build detection engineering and threat hunting tooling while setting technical direction for the team.

- 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
- Engineered a 'user activity tracker' that correlates enterprise telemetry to accelerate incident triage and proactive threat hunting
- Automated end-to-end quarantine email release across Microsoft 365 and Abnormal, cutting analyst response time on phishing and malicious mail
- Own enterprise security automation, AI development, and SIEM/logging architecture across the security program
- Set secure-coding and cybersecurity-forward AI usage standards; mentor engineers and advise leadership on detection engineering investments

Senior Information Security Consultant Confidential, Remote *Jan 2025 – Mar 2026*

Contract consulting role delivering hands-on security engineering, SOC operations, and vulnerability management for defense, fintech, and MSSP clients.

- Ran SOC operations for a US Defense Space market supplier across multiple Microsoft tenants
- Managed the Vulnerability Management Program for one of the largest US fintech clients using Qualys
- Restructured SOC workflow and trained analysts at an MSSP
- Designed secure architectures and provided compliance guidance (HIPAA, PCI-DSS, GDPR, NIST 800-53)

SOC Technical Manager → SOC Director → Director of Automation Compuquip Cybersecurity, Tampa/Doral, Florida *Jan 2021 – Dec 2024*

Progressive technical and leadership roles culminating in Director of Automation, owning AI development and security automation for MSSP clients.

- Built automation handling 3,500 tickets weekly, closing 47% without human involvement
- Owned all AI development in a secure MSSP environment — AI-powered security automation using Python, AWS Lambda, LLMs, and SOAR platforms
- Designed prompt engineering frameworks and AI guardrails ensuring safe, accurate, 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 including model evaluation, output validation, and security controls for LLM deployments

- Grew SOC client base from 16 to 52 customers and improved margin from 18% to 52% while leading a 17-person SOC, Red Team, and DFIR org

Sr. Cyber Security Architect Travel Syndication Technology (TST), Alpharetta, Georgia *Apr 2020 – Jan 2021*

Owned security architecture, detection tooling, and compliance across the organization.

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

Cyber Security Engineer → Senior Cyber Security Engineer Intercontinental Exchange, Marietta, Georgia *Aug 2018 – Apr 2020*

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

- Lead investigator on critical incidents; ran multi-server compromise investigations across three teams
- Led malware analysis in sandboxed environments and mentored junior analysts
- Designed security data flow pipelines and automated SOC triage tooling

IT Leadership & Systems Administration Roles Earlier Experience *Jan 1999 – Aug 2018*

Progressive IT and technical leadership roles, including Technical Services Manager at the National Wild Turkey Federation — led 8 technicians and developers supporting 300+ staff, saved \$50,000+/year migrating 3rd-party tools in-house, and owned web/network/application security. Earlier: 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, 2020

GCFA - Forensic Analyst, GIAC, 2019

GCIH - Incident Handler, GIAC, 2018

Lethal Forensicator Coin Winner, SANS/GIAC, 2019

SANS Challenge Coin for excellence in digital forensics

Associate in Network Administration, Virginia College, 2014 – 2016

GPA: 4.0

Technical Skills

AI/ML Engineering & Automation: LLM Integration, RAG Systems, Prompt Engineering, Agentic AI, AI Security & Guardrails, AI Governance, Model Evaluation, AWS Bedrock, AWS Lambda, Python Automation, Custom SOAR Development

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

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

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

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

Leadership & Mentorship: Technical Leadership, Engineer Mentorship, MSSP Operations, Team Leadership (17+ reports), Vendor Negotiations