

Phillip Tarrant

Cybersecurity Director | Automation Leader

ptarrant@gmail.com • (706) 294-6733

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

Accomplished and analytical professional with 20+ years of experience in cybersecurity, server infrastructures, and data-center operations. Proven expertise in Cyber Operations, digital forensics, penetration testing, information system management, malware reversing, threat detection, and threat hunting with and without AI integration. Proactive leader with a proven record of managing multiple large teams and leading the charge to complete project goals. Managed MSSP operations for 50+ large business clients encompassing over 150,000 assets and 1 million+ users.

Career Experience

Senior Information Security Consultant Confidential, Remote *Dec 2024 – Present*

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, 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
- Developed AI-powered security automation using Python, AWS Lambda, and SOAR platforms

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: Splunk, ELK Stack, Microsoft Sentinel, Microsoft Defender, Sentinel One, Rapid7 IDR, Stellar Cyber

SOAR Platforms: Swimlane, D3 SOAR, Torq, Playbook Development, Workflow Automation

EDR & Threat Detection: Darktrace, Tanium, Vectra, FireEye, Sentinel One, Detection Engineering

DFIR & Forensics: Volatility, Malware Analysis, Reverse Engineering, Incident Response, Evidence Collection, Multi-host Investigation

Penetration Testing & Red Team: Metasploit, Web Application Security, Attack Simulation, Red Team Oversight, Purple Team Testing, Vulnerability Assessment

Cloud Platforms & Security: AWS, Azure, Oracle Cloud, Lambda, EC2, Cloud Security Architecture, Hybrid Environments

AI/ML & Automation: AWS Bedrock, Large Language Models, RAG, Machine Learning, Python Automation, Custom Tool Development

Programming & Scripting: Python, PowerShell, Bash, SQL, YAML

Infrastructure & Systems: Windows Server, Linux/UNIX, Active Directory, VMware, Docker, Kubernetes, Network Architecture

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

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