TERRILL HILLIARD

IT Support & Systems • Security Operations • Endpoint / IAM Administration

Open to Fully Remote, Hybrid, Onsite, or Relocation • Available Immediately

terrillhilliard96@gmail.com | 818-934-0699 | linkedin.com/in/terrillhilliard

PROFESSIONAL SUMMARY

IT support and security operations professional with 5+ years across enterprise technical support, endpoint and identity administration, and security monitoring. Recently completed an M.S. in Cybersecurity & Information Assurance and actively seeking a new opportunity. Proven record as a Tier 2/3 escalation lead supporting 260+ users, automating ticket and asset workflows, and applying SIEM-based threat detection and vulnerability management. Combines hands-on troubleshooting with a data-driven, process-improvement mindset and strong end-user communication.

EDUCATION

M.S., Cybersecurity & Information Assurance Completed 2026

Western Governors University

B.S., Finance & Accounting

Wingate University

CERTIFICATIONS

CompTIA CySA+ • CompTIA PenTest+ • ISC² Certified in Cybersecurity (CC) • CompTIA SecurityX (In Progress)

TECHNICAL SKILLS

IT Support & Systems: ServiceNow ITSM • Jira • Windows 10/11 • macOS • Microsoft 365 (Teams, Exchange, SharePoint) • Microsoft Intune (MDM) • Active Directory / Entra ID • Endpoint Troubleshooting & Configuration

Security Operations: SIEM (Splunk, Elastic, CrowdStrike, Okta, Palo Alto) • Incident Response (NIST 800-61) • Log Correlation & Analysis • Threat Hunting • Security Audit & Compliance Monitoring

Hardware & Asset Management: IT Asset Lifecycle • Device Inventory Tracking & Auditing • Break-Fix & Replacement • Provisioning & Onboarding • Printers & Peripherals • MDM

Vulnerability & Pen Testing: Nessus • OpenVAS • Metasploit • Burp Suite • Nmap • Nikto • SQLMap • Vulnerability Assessment & Remediation

Cloud & Infrastructure: Microsoft Azure • Prisma Access • Zero Trust (NIST 800-207) • Firewall Configuration • VPN Management

Automation & Data: Python • PowerShell • Bash • SQL • Dashboarding & Reporting

Frameworks & Standards: MITRE ATT&CK • NIST 800-53/61/207 • ISO 27001 • FedRAMP • Change Management

PROFESSIONAL EXPERIENCE

Systems Analyst May 2025 – Jan 2026

Relias | *Morrisville, NC (Hybrid, Contract)*

- **Escalation lead across 260+ users —** served as hands-on technical lead and Tier 2/3 escalation point, guiding junior staff on hardware requests, break-fix triage, and provisioning while owning complex incidents end-to-end.
- **Endpoint & identity administration —** administered Microsoft Intune (device enrollment, compliance policies, app deployment, security baselines) across Windows and macOS; managed access and endpoint compliance via Azure AD / Microsoft Entra.
- **Onboarding & service delivery —** led laptop/workstation setup and new-hire onboarding; managed ServiceNow ITSM queues and prioritized work by business impact, keeping the team focused on highest-urgency issues.

- **Automation —** built PowerShell automation for ticketing and asset workflows, cutting manual processing time and improving operational efficiency; maintained accurate multi-site hardware inventory.
- **Infrastructure projects —** supported large-scale printer/MFD replacements, Windows 10→11 upgrades, device-lifecycle automation, and warehouse barcode/label peripherals across multiple sites.

Technical Support Specialist
Jan 2023 – Feb 2025

Trajector Medical | *Remote*

- **Enterprise endpoint support for 200+ users —** supported mission-critical systems, PC/Mac desktops, laptops, mobile devices, and printers; processed hardware requests and break-fix/replacement workflows.
- **Reduced resolution time 30% —** applied SQL queries and systematic troubleshooting to diagnose and resolve complex issues faster.
- **Security monitoring —** used Splunk SIEM for log analysis and event monitoring, building custom dashboards and alerts to surface anomalous activity.
- **High-volume queue management —** triaged hardware/software incidents in Jira and ServiceNow against SLA targets while maintaining a strong end-user experience; partnered with security and engineering on compliance posture.

Cybersecurity Specialist (promoted from BDR)
Jul 2020 – Dec 2022

Sennovate | *Remote*

- **Promoted into a technical role —** advanced from a client-facing position to Cybersecurity Specialist based on demonstrated technical aptitude.
- **Cut critical-finding exposure 40% —** conducted 50+ vulnerability assessments using industry-standard tools and drove NIST-aligned remediation.
- **IAM / MFA rollouts for 15+ clients —** supported identity governance deployments that reduced unauthorized-access incidents across distributed environments.
- **SIEM analysis —** performed log correlation to identify potential incidents and contributed to threat analysis and security-control validation.

Data Analyst
Jun 2019 – Jul 2020

Wells Fargo | *Silver Spring, MD (Onsite)*

- **Analyzed 10M+ records —** generated insights supporting strategic, risk-management, and regulatory-reporting decisions across business units.
- **Leadership dashboards —** built 10+ interactive dashboards adopted by senior leadership to track KPIs and accelerate reporting cycles.
- **Data integrity —** developed complex SQL to extract, transform, and validate enterprise data; supported audit and compliance documentation.

PROJECTS & LAB WORK

- **Home SOC Lab (Elastic SIEM + Kali Linux) —** built a virtualized attack/defend lab; ingested endpoint logs, authored detection rules, and investigated simulated intrusions end-to-end.
- **Vulnerability Assessment Capstone (WGU M.S.) —** ran a full-scope assessment with Nessus and OpenVAS, producing an executive risk report mapped to NIST 800-53 controls.
- **TryHackMe / HackTheBox —** active in CTF-style offensive/defensive challenges reinforcing privilege escalation, lateral movement, and SIEM detection aligned to MITRE ATT&CK.