Tony Le

TONYHUYLE123@gmail.com · (832) 507-4580 · tonyhuyle.com

Professional Summary:

Security-focused IT professional with hands-on experience in IT support, Active Directory administration, and cybersecurity labs focused on SIEM monitoring, threat detection, authentication analysis, and incident triage. Skilled in analyzing security logs, investigating suspicious activity, and documenting findings using Splunk, Microsoft Sentinel, and Windows security tools. CompTIA Security+, CySA+, Network+, A+, and Microsoft SC-300 certified.

Technical Skills:

Security Skills: SIEM, Log Analysis, Threat Detection, Incident Triage, IDS/IPS, Vulnerability Assessment, IAM Security
Identity & Infrastructure: Active Directory, Microsoft Entra ID, Okta, RBAC, SSO, MFA, DNS/DHCP, TCP/IP, Authentication
Tools & Environments: Windows, Windows Server, Splunk, Azure, Microsoft Entra Admin Center, Wireshark, Jira, PowerShell
Certifications: CompTIA A+, Network+, Security+, CySA+, SC-300

Work Experience:

Help Desk Technician| Triple-S Steel Supply **July 2026 – Present**

- Resolve and document service requests and incidents across hardware, software, networking, Microsoft 365, user access, and enterprise ERP systems through remote and on-site troubleshooting
- Provision and administer user accounts and access across Active Directory and Microsoft Entra ID in a synchronized hybrid identity environment, including onboarding, password resets, MFA, and access management.
- Manage the lifecycle of company endpoint devices, including asset inventory, imaging, configuration, deployment, troubleshooting, and equipment replacement.
- Administer Microsoft 365 services, including user licensing, mailbox management, and access administration.

Technical Support Representative| Ace Pay **September 2025 – July 2026**

- Investigated and resolved access, configuration, connectivity, device, and service availability issues affecting operations.
- Managed support incidents and service requests in Jira, documenting investigation steps, escalations, resolutions, and user communication through closure.
- Configured and deployed POS terminals and SaaS payment solutions while troubleshooting connectivity, software, and device-related issues.

IT Technician (Contract) | DUG – DownUnder GeoSolutions **October 2025 – October 2025**

- Supported the relocation of 600+ Linux HPC server nodes across data centers, assisting with hardware migration, system handling, and infrastructure continuity.
- Diagnosed and repaired server hardware issues involving memory, processors, and power supplies to restore functionality.
- Tracked and documented server components, fiber-optic cabling, and networking equipment to maintain accurate infrastructure inventory.

Project Experience:

Cloud IAM Security Lab: Microsoft Entra ID P2, Okta, SAML, MFA, Conditional Access

- Managed identities, groups, and application access in Microsoft Entra ID and Okta for a simulated enterprise environment
- Implemented RBAC, SAML-based SSO, MFA, and Conditional Access policies to enforce least privilege access
- Investigated authentication activity, group membership changes, and access events using Entra sign-in and audit logs
- Performed access reviews, lifecycle management workflows, and administrative role delegation to support identity governance

Network Infrastructure & Security Monitoring Lab: pfSense, VMware, Splunk, DNS/DHCP

- Designed and deployed a segmented virtual network using pfSense to manage WAN/LAN traffic and communication
- Integrated Splunk SIEM to centralize Windows Security logs for authentication monitoring and event analysis.
- Simulated brute force attacks and analyzed logs to identify repeated failed credential validation attempts
- Diagnosed and resolved network and security issues including IP conflicts, DNS failures, and authentication anomalies using ping, nslookup, and Splunk queries

Active Directory IAM Lab: VirtualBox, Windows Server, Group Policy, PowerShell

- Managed identity lifecycle operations including provisioning/deprovisioning, password resets, and privilege changes
- Implemented Group Policy to enforce authentication controls and restrict unauthorized system access
- Automated account management processes using PowerShell, improving consistency and reducing risk of misconfiguration

RDP Honeypot Lab: Azure, PowerShell, KQL, Microsoft Sentinel

- Captured over 1,000 real-world brute-force attempts by deploying a honeypot VM in Azure
- Enabled real-time detection and response by integrating Microsoft Sentinel with KQL dashboards
- Improved threat visibility and incident tracking by forwarding logs to a centralized SIEM

Education:

University of Houston
Bachelor of Science, Computer Science **Graduated May 2025**
Minor in Mathematics GPA: 3.3