John Tyler

IT Support Specialist | Windows 11 | Microsoft 365 | Active Directory | ServiceNow
j.tyler.pro@gmail.com | linkedin.com/in/john-ty-tech | github.com/johninfra

PROFESSIONAL SUMMARY

CompTIA A+ and Security+ certified IT Support professional with experience supporting 30+ Windows endpoints and over 200 Microsoft 365 users. Skilled in Tier 1/Tier 2 troubleshooting, Windows administration, account access, password and MFA support, software issues, networking, and remote user assistance. Experienced managing ServiceNow tickets, documenting root causes and resolutions, escalating complex incidents, and delivering responsive end-user support. Hands-on labs reinforce Windows Server, Active Directory, Azure, PowerShell, and security operations.

CERTIFICATIONS & EDUCATION

CompTIA Security+ | CompTIA A+
California Institute of Applied Technology | A.S., Computer Information Systems | May 2026

PROFESSIONAL EXPERIENCE

IT Support Specialist | Oatridge Security Group | 2023 - 2026

- Supported 30+ Windows endpoints and over 200 Microsoft 365 users, resolving workstation, account, application, printing, and connectivity issues across headquarters and client sites.
- Troubleshot Windows 10/11, Microsoft 365, Active Directory and Entra ID sign-ins, password resets, MFA enrollment, user provisioning, security groups, and access requests.
- Owned incidents in ServiceNow from intake through troubleshooting, resolution, documentation, escalation, and follow-up; communicated technical steps clearly to end users.
- Diagnosed DNS, DHCP, VPN, TCP/IP, and endpoint issues using Event Viewer, PowerShell, command-line utilities, and Windows administrative tools.
- Validated fixes, recorded reproducible diagnostic evidence, and partnered with higher-tier teams to address persistent system and network issues.

Security Operations & Access Control Specialist | VIP Access Management | 2021 - 2023

- Provided frontline support for employee, contractor, and visitor credential and access issues, including verification, provisioning, updates, and deactivation.
- Investigated access incidents, reviewed logs, documented findings, and escalated operational or security issues to the appropriate teams.
- Processed authorized access changes accurately, maintained detailed records, and communicated status and resolution to affected users.

PROJECTS

Azure Enterprise Administration Lab | GitHub
Built and managed Azure virtual networks, subnet NSGs, Azure RBAC, policy assignments, resource locks, monitoring alerts, and a Windows Server 2022 VM; validated DNS, HTTPS, and Windows configuration with PowerShell.

Azure Windows Diagnostic Automation Workflow | GitHub
Created a GitHub Actions workflow to execute Windows diagnostic checks and publish an HTML troubleshooting report, emphasizing repeatable investigation and support documentation.

Microsoft Entra MFA & RBAC Lifecycle Lab | GitHub
Practiced account and group administration, MFA registration, Azure role assignments, sign-in verification, permission revocation, and least-privilege support workflows.

Splunk SIEM Security Monitoring Lab | GitHub
Analyzed 69,631 Windows Security and Sysmon events; developed searches and dashboards for authentication failures, PowerShell activity, and suspicious processes.

IT Support & Cybersecurity Lab Portfolio | GitHub
Built and documented 26+ hands-on labs covering Windows Server, Active Directory, Entra ID, Microsoft 365, endpoint administration, networking, Linux, remote support, and PowerShell automation.

TECHNICAL SKILLS

End-User Support: Windows 10/11, Desktop Troubleshooting, Software Installation, Printer Support, Remote Support, Ticket Documentation, ServiceNow
Microsoft Administration: Microsoft 365, Active Directory, Microsoft Entra ID, User/Group Management, Password Resets, MFA, Windows Server, Group Policy, SAML SSO, SCIM User Provisioning (Entra ID)
Networking & Diagnostics: TCP/IP, DNS, DHCP, VPN, Wi-Fi, Event Viewer, PowerShell, Command Prompt, Wireshark, Nmap
Cloud & Security: Azure Administration, Azure RBAC, Azure Monitor, Endpoint Security, Splunk, Windows Security Logs, Sysmon
Additional Tools: VMware Workstation, Git, GitHub, Ubuntu Linux, Kali Linux, Microsoft Graph PowerShell