Curtis Johnson
Ph: 605-651-1213
https://www.linkedin.com/in/curtisljohnson/
Website: https://yourtech.online/

Professional Summary

Aspiring Cybersecurity Specialist with 8 years of IT experience, including 1 year in network operations, Windows and Linux server administration. Skilled in security monitoring, incident response, and leveraging SIEM tools. Experienced in managing Active Directory, automating scripts with PowerShell and Bash with a strong foundation in vulnerability management, threat remediation, network troubleshooting and asset management. Committed to secure IT infrastructures and improving response efficiency while reducing downtime.

Key Skills

- **Threat Detection & Response**: Malware removal, phishing, security incidents
- **SIEM Tools**: Correlation analysis, Security Monitoring, Reporting, alerts, SPL/Splunk
- **Threat Hunting**: TTP & Analysis, IOC Collection, KQL, Azure Data Explorer, MITRE & Attack
- **Threat Intelligence**: Qualys, MS Defender XDR, threat analysis
- **Incident Response**: Root cause analysis, Containment and mitigation
- **Security Monitoring**: Log analysis, network traffic monitoring, packet analysis
- **Vulnerability Management**: Patching, Qualys, ServiceNow, Asset Management
- **Automation & Scripting**: PowerShell, Bash, troubleshooting automation scripts
- **System Administration**: Windows/Linux servers, AD, firewall troubleshooting
- **Tools & Technologies**: Wireshark, ProcMon, Netstat, Ethtool, pcap, Digital Guardian

---

Certifications

- FEMA - Basic incident Command System for Initial Response – April 2025 – April 2028
- KC7 – Frognado in Valdoria, Rap Beef, Scandal in Valdoria, Titan Shield, Valdoria Votes
- Splunk Core Power User – August 2024 to August 2027
- CompTIA Pentest+ – January 2024 to January 2027
- CompTIA CySA+ – November 2023 to January 2027

- CompTIA Security+ – December 2020 to November 2026
- CompTIA Network+ – December 2020 to November 2026
- Qualys VDMR – June 2023
- ICF Certified Trained Coactive Coach

Professional Experience

WATG/Vaco – Tustin, CA *January 2025 – Present*
Helpdesk Technician (Contract)

- Monitor and triage tickets to global staff.
- Manage Tustin IT services for site while providing remote support for 4 domestic sites.
- Mentor and support staff domestically and globally.
- Mentor technicians – network troubleshooting, sla adherence, accountability, threat deterrence, process improvement, procedures, IT service delivery, asset and inventory management.
- Advise management – team communication, IT service delivery, asset utilization, sla adherence on contractor deployments and loaner deployments.
- Enhance confidence while manage expectations with staff – disk management, deployments, printers, design application performance, hardware and onboarding.
- Through PI, Increase domestic deployments and onboarding effectiveness by 40%.
- Create PowerShell scripts to automate deployments, reduce deployment time by 30%.
- Enable Improved IT workflows resulting in increased confidence from business staff.
- Vendor management, Asset management, Hardware repair, conference room and printer support, Windows maintenance, architecture software support.
- Advise and teach business staff on security hygiene related to hardware, software and data.
- Advise on phishing threats, email analysis/delivery and Mimecast support.
- Provide VPN/ Remote connection support for WFH staff.
- Troubleshoot mobile devices while providing mfa support and setup.
- AD/group policy troubleshooting
- Create and adapt documentation for IT operations and business users.

Luskin OIC/Robert Half – LA, CA, *March 2023 – April 2023*
Desktop Technician (Contract)

- Managed ticket que, triaged and provided direct coaching on tickets with 95% customer satisfaction.
- Increased ticket resolution rate by 75% in small team.
- Supported endpoint security and user accounts, including AD account creation and MFA setup.

- Automated security processes with PowerShell, improving audit and file management processes.
- Handled VPN, Citrix, and firewall troubleshooting to secure remote work infrastructure.
- Performed device hardening and endpoint attack vector audits.

Vubiquity/Robert Half – Burbank, CA, *May 2022 – February 2023*
NOC Technician (Contract)

- Managed ticket que, triaged and provided 1st line of defense while providing direct coaching on tickets. Coached staff on priority SLA adherence utilizing Jira.
- Incident commander for critical domestic after-hours events, reducing MTTR by 40%.
- Responded and contained security breaches, advised on chain of command and accountability, lessons learned while documenting incident reports and briefing.
- Maintained NOC facility, situational awareness and logistics while liaising with SysEng.
- Influenced change management procedures for managing priority 1 incidents.
- Enhanced security posture through process improvements and fine-tuning of false positive alerts.
- Audited and supported security controls in line with ISO 27001 for cloud and on-prem environments.
- Provided initial setup, training and written procedure for content quality monitoring tool.
- Influenced and evaluated shift change over procedures enhancing communications.
- Evaluated and reported MS internal incident response procedures for cloud instances per service category and defined maintenance agreements.
- Established documentation and outline process for monitoring customer sites and data anomalies.

Fortra – Glendora, CA, June 2021 – February 2022
Server Support Analyst

- Managed ticket que, coded and triaged tickets.
- Provided 90% customer satisfaction while closing 9+ (L1, L2 & L3) tickets per day.
- Advised Administrators on server maintenance and security.
- Conducted packet analysis using Wireshark.
- Advised on incident response for account access attempts and DOS.
- Assisted in mitigating threats such as Log4j vulnerabilities and advised clients on preventative controls.
- Engaged in network troubleshooting using tools like ProcMon and Procdump and addressed security issues in hybrid environments.

Pankow Builders/Modis – Pasadena, CA, *August 2019 – May 2020*
Helpdesk Technician (Contract)

- Monitored and remediated security incidents such as phishing attacks, improving workforce reporting accuracy by 95%.
- Provided 20+ (L1 & L2) ticket closures per day with 90% customer satisfaction rating.
- Provided remote support for branch offices, resolving network and VPN issues during WFH transition.
- Enhanced endpoint security through device auditing and remediation.

S & L Computers – Fargo, ND *November 2018 – March 2019*
Junior System Administrator

- Provided 10+ ticket closures per day for small business customers.
- Responded to phishing incidents, providing advisement and remediation across multiple client environments.
- Administered endpoint patching, malware defense, and server configurations.

Education

Bachelor of Science in Electronic Engineering Technology
South Dakota State University