Ty Johnson

PRINCIPAL SECURITY ENGINEER

Eden Prairie, MN · 0tyjohnson0@gmail.com · 612.555.5555 · linkedin.com/in/handle · github.com/handle

PROFILE

Principal Security Engineer with **28+ years** of enterprise technology leadership and stewardship.

Demonstrated expertise in multiple security and technology domains.

Adept technology practitioner with confident skill-sets on multiple platforms and systems.

Career trajectory reflects expanding scope and deepening complexity, anchored by a consistent record of successes directing enterprise technology — from strategy through delivery and operational support — across multiple large enterprises.

CURRENT PROJECT WORK

> *Spearheading the use and integration of AI capabilities into Cybersecurity Engineering operations and analytics. Using GitHub Copilot with MCP tooling to cross-reference, correlate, and reconcile complex data joins between Microsoft Defender and Palo Alto Firewall rule-sets and logs, as part of a larger enterprise network segmentation project.*

CORE COMPETENCIES

PKI & Identity — Certificate Lifecycle Management · ADCS · Offline Root CA · Venafi (CyberArk) · Azure Key Vault · GlobalSign · F5 · Enterprise SSO · Entra ID / Azure AD

Security Awareness & GRC — KnowBe4 · Phishing Simulation · Security Awareness Programs · Compliance Training · TPRM · ISO 27001/27002 · Zero Trust · ITSM · NIST SP 800 Series

Cloud & Infrastructure — Microsoft Azure · Microsoft Security · Microsoft 365 · Cisco Umbrella · Hyper-V · Virtualization · Windows Server · Linux · Network Security · Switching & Routing

Tooling & Automation — PowerShell · Git · GitHub Copilot · GenAI / RAG · Jira Service Management · Python Scripting & Automation · Claude Code · DeepSeek v4 · MCP

Detection & SecOps — SIEM Engineering · Threat Hunting · Behavioral Detection · Incident Response · Threat Intelligence · Alert Engineering & SOAR · Playbook Development · NIST CSF 2.0 · CIS v8

EXPERIENCE

Sr. Cybersecurity Engineer

C. H. Robinson Worldwide

Eden Prairie, MN · Oct 2021 – Present

Scope: Senior-level IC on a dedicated Cybersecurity Engineering team inside a Fortune 200 global logistics company (~16,000 employees, operations in 37 countries). Mostly remote work, with some datacenter visits. High degree of autonomy; multiple scrums weekly.

Description: Modernized and automated a complex, legacy PKI ecosystem across a Microsoft/Azure-centric enterprise, significantly improving certificate lifecycle management, security posture, and operational efficiency. Manage the operations and continuous improvement of the enterprise Cybersecurity Awareness program, encompassing mandatory compliance training, phishing simulation campaigns, and targeted privileged-user training tracks. Technology and Security initiatives in direct support of NIST CSF V2 and CIS v8 polices, standards, and controls. Security consulting with peer technology and engineering Teams.

PKI / CERTIFICATE LIFECYCLE MANAGEMENT (2023 – PRESENT)

- Eliminated **2–4** annual certificate-caused outages by leading a 3-year enterprise PKI modernization: rebuilt Offline Root CA onto a cost-optimized, air-gapped high-availability architecture, reducing root-CA infrastructure costs by **~50%** (**~$8K** → **~$4K**) while improving physical security posture and shrinking the attack surface.
- Recovered **~600** engineering hours per year by implementing Venafi certificate automation on F5 load balancers, removing the manual cert-lifecycle bottleneck across **~1,500** managed certificates.
- Deployed 2 new purpose-segregated internal Issuing CA servers and unified public + private PKI lifecycle by integrating GlobalSign (public CA) alongside ADCS via Venafi, creating a single-pane cert-management surface.
- Initiated Azure Key Vault automation to extend lifecycle management into cloud-native workloads, eliminating a class of manual secret-rotation risk.
- Accelerated and de-risked the Offline Root CA deployment by grounding GitHub Copilot on internal PKI documentation (RAG-based), cutting deployment planning time and reducing config-error exposure.
- Engaged directly with PKI engineering leads at Microsoft and Venafi to resolve architecture gaps; led enterprise-wide technical briefings on TLS industry changes (shortened certificate validity windows).

NETWORK SEGMENTATION & TRAFFIC LEGITIMIZATION (2026 – PRESENT)

- Collaborating on the company's first-ever enterprise network segmentation program — a multi-year Zero Trust initiative affecting all **~16,000** users across a historically flat network topology; one of the largest technology projects in company history.
- Accelerating traffic legitimization (whitelist-build) by deploying AI to analyze network flows and Microsoft Defender workstation logs at scale, generating technical narratives that compress weeks of manual classification into structured, reviewable output.

AI OPERATIONALIZATION (2025 – PRESENT)

- Leading the adoption of AI-assisted engineering workflows across the Cybersecurity Engineering team — developing project-based and task-based GitHub Copilot workflows, prompt libraries, and environment configurations that measurably improve team output.

SECURITY AWARENESS & PHISHING SIMULATION (2022 – PRESENT)

- Drove enterprise phish-prone percentage (PPP) from **8–10%** down to **2–5%** — a sustained, year-over-year reduction across all **~16,000** employees — by owning the full KnowBe4 security awareness and phishing simulation program, including monthly simulations with automated closed-loop remediation for anyone who fails.
- Scaled the program to test every population group (including privileged/high-risk users) at minimum quarterly cadence, with targeted campaigns for elevated-risk cohorts.
- Designed and runs the annual Cybersecurity Awareness Month (October) campaign — interactive content, games, and prize-based incentives — driving org-wide engagement and positive security behavior reinforcement.
- Administers annual Corporate Compliance Month training portfolio, ensuring **100%** of **~16,000** employees complete required security awareness coursework.

ENTERPRISE SSO (2022, COMPLETED)

- Delivered enterprise SSO on Azure Entra, onboarding 50 applications and sites to centralized identity management; responsibility subsequently redistributed as the program matured.

THIRD PARTY RISK MANAGEMENT (TPRM) (2022, COMPLETED)

- Stood up the third-party vendor risk management process in early Phase 2; transitioned ownership to a dedicated department once the program was operational.

SOC Analyst

C. H. Robinson Worldwide

Eden Prairie, MN · Jun 2019 – Oct 2021

Scope: Build and operationalize the company's first Security Operations Center. Develop SIEM/SOAR functionality, build-out investigative workflows, and further develop detection capabilities.

- Co-engineered the company's inaugural SOC and SIEM/SOAR (LogRhythm). Built alert rules, behavioral detections, incident management workflows, and operational playbooks while simultaneously operating the live environment.
- Built behavioral detection models by baselining normal human behavior, network traffic, and system-resource patterns, then engineering alert rules on deviations; integrated threat-intelligence feeds (Anomali ThreatStream · Cisco Umbrella) for real-time situational alerting.
- Automated alert adjudication, incident creation, and tiered escalation/notification using PowerShell, reducing analyst toil and accelerating response throughput.
- Authored the full library of operational, scenario-based, and incident-based playbooks; documented all SOC workflows and processes from scratch (greenfield — no prior documentation existed).
- Helped staff and scale the SOC to a global follow-the-sun model; interviewed approximately 24 analyst candidates over 18 months to build out the international team.
- Aligned SOC operations to NIST CSF 2.0 and CIS v8; collaborated cross-functionally with corporate and technology departments to develop policy, standards, and escalation workflows.

Information Security Analyst

Minnesota State Lottery

Roseville, MN · 2018 – 2019

Scope: Sole practitioner securing the state lottery's information systems inside one of the most heavily regulated and audited government-adjacent environments in Minnesota.

- Developed and enforced information security strategies, policies, and technical standards in a high-governance, heavily regulated environment — demonstrating security-program ownership under rigorous compliance scrutiny.
- Conducted technical security reviews of business and information systems; ensured security posture met state and industry regulatory requirements.
- Operated a LogRhythm SIEM environment, applying detection and analysis skills developed through hands-on SIEM engineering.

Network Security Engineer

University of Minnesota, Office of Information Technology

Minneapolis, MN · 2017 – 2018

Scope: Technical SME for a $14M enterprise firewall and UTM modernization — part of an $80M network infrastructure overhaul — impacting the first core-network rebuild across the U of M system in 25 years.

- Served as primary technical SME for a **$14M** enterprise firewall/UTM deployment spanning **~70,000** endpoints across four campuses (Twin Cities, Duluth, Rochester, Morris) — the first overhaul of the university's core network in 25 years.
- Designed logical firewall and UTM policy architecture, led data-center firewall equipment deployment, and collaborated with multiple technology teams and vendors to debug platform performance issues and resolve hardware/software defects.

IT Infrastructure Manager

Boynton Health, University of Minnesota

Minneapolis, MN · 2010 – 2017

Scope: Managed IT Service Desk and Infrastructure groups (9–12 FTE) supporting ~600 endpoints and ~85 servers in an academic healthcare environment.

- Remediated 19 essential IT audit findings in 18 months following a University of Minnesota internal audit — demonstrating structured, accountable execution under external scrutiny.
- Orchestrated the full physical relocation of the enterprise IT data center and systems, managing risk, continuity, and coordination across multiple stakeholder groups.
- Contributed to ISO 27002 committee work in support of the University's ISO 27001 program, applying international security-standard methodology to institutional governance.
- Led and developed **9–12** FTE across IT Service Desk and Infrastructure; drove hiring, mentoring, performance management, and career growth for the team.

Earlier Career — Sr. Systems Engineer

Mystic Lake Casino Hotel

Prior Lake, MN · 2002 – 2010

Built foundational IT operations and systems-management expertise in a 24/7/365 high-availability environment (~3,500 employees, ~5,000 endpoints, 7,500–30,000 daily guests, 350-room hotel).

Technologies: Oracle · MS SQL · UNIX · Micros (Hospitality POS) · Property Management System (PMS) · Electronic Payment / Card Processing · Document Imaging · Windows Server · Virtualization · Patch Management

Career origins (1998–2002): Entered enterprise technology at Decision One (Sr. Support Specialist — Tier-2 support, staff training, and QC across a national 24/7 call center) and US Bancorp Piper Jaffray (Technical Support — online trading-system QA and desktop support; designed and managed a multi-platform Windows/Linux/Mac test lab) — the foundation of a 28-year climb from the support desk to principal-level engineering.