

Justin Knox, CISSP, CISA

Phone: +1 (313) 824-8535
Email: jtknox@posteo.de

SUMMARY

Cybersecurity & infrastructure engineer with 20+ years experience. Skilled in vulnerability remediation, systems hardening, and hybrid system integration. CISSP- and CISA-certified, with a proven record of building resilient, compliant architectures using FOSS tools and automation.

Featured Employers: Google | British Telecom | Scientific Games

RELEVANT EXPERIENCE

- 10.2024 – Present DTE Energy, Cyber Security Analyst
Gas Cybersecurity Compliance | Strategic Staffing Solutions
Detroit, MI | 40% remote
- Implemented vulnerability management (VM) operations across hybrid IT/OT environments, updating full system remediations (FSR) based on manually calculated CVE and CVSS scores, tracking remediation via SLA-compliant workflows, and reporting risk posture to leadership.
 - Worked with network engineering teams, integrating TLS, IPsec, and 802.1X protocols with RBAC and ACLs to safeguard mission-critical traffic across segmented networks.
- 09.2023 –10.2024 Great Lakes Water Authority, Senior IT/OT Infrastructure Administrator
Cyber & Information Security, Water Resource Recovery Operations
Detroit, MI | Onsite to 20% Remote
- Built and deployed a centralized cyber defense platform integrating SIEM, CMDB, and IPAM (PostgreSQL, Redis, Jenkins) across segmented IT/OT environments.
 - Designed and implemented a clustered Debian/Red Hat Linux virtualization environment with automated provisioning, patching, and sustainment pipelines using PowerShell and Bash, aligned with NIST 800-53, CSF 2.0, and Zero Trust principles.
 - Supported SCADA and DCS modernization efforts through collaborative field operations engagement, troubleshooting hybrid control system architectures, and optimizing database workflows across multi-vendor environments consistent with asset management methodologies.
 - Deployed TLS 1.2 and X.509 certificate frameworks to secure communication channels between DMZ-layer applications.
 - Developed (non-GPT) Active Directory security auditing and reporting solutions, using real-time network diagnostics from Cisco; and change-management for Microsoft 365.
- 06.2023 – 09.2023 Corewell Health, Systems Engineer
Critical Environment Engineering | Matech Resources, LLC
Grand Rapids, MI | Onsite to 20% Remote
- Streamlined production infrastructure deployment, cutting delivery time by 40% through workflow optimization and bottleneck elimination.
 - Applied industry-standard deployment methodologies, enhancing scalability, reliability, and maintainability of infrastructure rollouts.
 - Identified and resolved critical infrastructure risks ahead of deployment, ensuring minimal downtime and maintaining operational continuity during rollouts.

| | |
|-------------------|---|
| 12.2018 – 12.2021 | Google, Senior Operations Engineer |
| | <i>Network Operations Server Operations Hardware Operations Engineering Field Services </i> |
| | <i>Data Center Infrastructure Operations Google Cloud VMWare</i> |
| | <i>Charleston, SC Reston, VA Washington DC 100% Onsite</i> |
| | <ul style="list-style-type: none"> - Deployed the East Coast's Google Cloud VMware Engine project, delivering 75% of milestones ahead of schedule by driving infrastructure readiness, workload isolation, and secure-by-default configurations across production systems — with emphasis on Linux-based environments modeled after Google's hardened Debian variants (e.g., gLinux), ensuring compatibility, stability, and policy enforcement at scale. - Developed automation tools (BASH, Python, G-SQL/BigQuery, Protobuf, gRPC, Borg/Kubernetes) to streamline server diagnostics and repair workflows, achieving over 800% recidivist cases and reducing manual repair intervention. - Awarded 19 Peer Bonuses and 2 Challenge Coins for excellence under pressure during Hurricane Dorian and the COVID-19 pandemic, demonstrating leadership and resilience in global operations. |
| 07.2017 – 12.2018 | Switch Inc., Data Center Technician |
| | <i>Network Operations</i> |
| | <i>Las Vegas, NV 100% Onsite</i> |
| | <ul style="list-style-type: none"> - Conducted physical penetration tests for high-profile data center clients, following initial work in smart-hands and rack deployments. - Automated ticket workflows with AutoHotKey, reducing processing time by 65%. |
| 10.2016 – 06.2017 | Pinnacle Community Services, Senior Systems Administrator |
| | <i>Las Vegas, NV 100% Onsite</i> |
| | <ul style="list-style-type: none"> - Designed and deployed HIPAA-compliant infrastructure using FOSS technologies, implementing hardened firewalls, encrypted storage, RBAC access controls, and secure IAM with TLS/SSH tunneling and network segmentation. - Conducted digital forensics and incident response in compliance with legal standards, applying encryption, key management, and containment strategies to ensure traceability, defensible posture, and audit-ready compliance. |
| 11.2013 – 04.2015 | Scientific Games (formerly Bally Technologies), Senior Technical Specialist |
| | <i>Technical Training and Documentation Department</i> |
| | <i>Las Vegas, NV 100% Onsite</i> |
| | <ul style="list-style-type: none"> - Developed and deployed the company's first internal training portal. - Implemented Nevada Gaming Control Board and New Jersey Division of Gaming Enforcement security protocols, documenting and distributing field operating procedures. - Developed and published the technical field service videos for Bally Technologies, WMS, and Shufflemaster products, including slot machines, card shufflers, roulette machines, and video poker systems, reducing travel-related training costs by 95%. |

| | |
|-------------------|---|
| 05.2008 – 09.2009 | <p>British Telecom (formerly Infonet), Senior Network Event Management Technician <i>Network Operations Center Network Event Management Center Global Converged Services, Network Event Management Center</i> <i>El Segundo, CA 100% Onsite</i></p> |
| | <ul style="list-style-type: none"> - Managed incident response for OSI L1-3 across MPLS & BGP, utilizing Cisco, Juniper, and Alcatel-Lucent platforms. - Developed OpenCV-based machine vision automation scripts to reduce incident resolution time from 4 hours to under 10 minutes, leveraging PowerShell and custom algorithms to enhance network monitoring and incident response. - Monitored and optimized TCP traffic for L1-L3 network performance on MPLS, BGP, and core platforms (Cisco, Juniper, Alcatel-Lucent), reducing latency with custom TCP optimizations and response time modification techniques. |
| 06.2006 – 11.2007 | <p>Synetcom Digital Inc., Junior Electronics Engineer <i>El Segundo, CA 100% Onsite</i></p> |
| | <ul style="list-style-type: none"> - Engineered industrial SCADA radios from PCB to application layer as part of the R&D team, including chip-level systems integration, embedded microcontroller development (PLC-to-RF encapsulation over RS-232/Ethernet), and GUI design using C and TKL. - Simulated field conditions in the lab to validate reliability and drive iterative improvements. |
| 03.2004 – 06.2006 | <p>DeVry University, Academic Tutor, Faculty Assistant & Lab Technician <i>Long Beach, CA 100% Onsite</i></p> |
| | <ul style="list-style-type: none"> - Supported academic success and hands-on learning as a faculty assistant and peer tutor in computer science, networking, and electronics. - Led one-on-one and group tutoring sessions, graded coursework, and assisted faculty in the advanced development lab—helping students build lab readiness, troubleshoot real systems, and translate theory into working projects. |

CONSULTING ENGAGEMENTS

| | |
|-------------------|--|
| 12.2021 – 03.2023 | <p>Startup CTO / Technical Consultant Alchemy Computing, Dumpt'd (Pre-revenue) — Washington, DC Remote</p> |
| | <ul style="list-style-type: none"> - Served as acting CTO for early-stage startup, leading a small engineering team in prototyping network infrastructure and full-stack architecture (Laravel, PostgreSQL). |
| 09.2009 – 11.2013 | <p>Technical Consultant (Independent) Alchemy Computing — Las Vegas, NV Onsite</p> |
| | <ul style="list-style-type: none"> - Delivered IT and network engineering services for SMBs in cosmetics and music production, including website development, malware remediation, and electronics prototyping (under NDA). |

PROJECTS

Homelab 4x Orange Pi micro-cluster running home automation VMs, with a Palo Alto PA-500 and 1Gb PoE Avaya L2 switch for VLAN segmentation and multi-cloud, offsite backup rotation for resilience. Proxmox cluster on Dell R610/R430 servers with Windows Server 2022 AD, DNS, SMB, and Linux dev/security VMs, utilizing a Cisco 1845 ASA for custom network security.

CERTIFICATIONS & TRAINING

| | |
|------------------|---|
| CISSP | Certified Information Systems Security Professional International Information System Security Certification Consortium (ISC2) Member ID: 954626 03.2024 - Present |
| CISA | Certified Information Security Auditor Information Systems Audit and Control Association (ISACA) Member ID: 2063351 11.2024 – Present |
| Security+ | Computing Technology Industry Association (CompTIA) Candidate ID: COMP001022411475, 11.2023 – Present |
| Technician Class | FCC Amateur Radio License Federal Communications Commission (FCC) Callsign: KF8BVZ 07.2024 – Present |
| OSCP | <i>Offensive Security Certified Professional</i> (IN PROGRESS) <i>Expected certification: September 2026</i> |

EDUCATION

| | |
|-------------------|--|
| 03.2003 – 03.2008 | Bachelor of Science in Computer Engineering Technology <i>DeVry University, Long Beach, California</i> Cum Laude, GPA: 3.6 |
| | - Best Senior Project 2008: "Fingertip Effects" (Acoustic Manipulation using Hand Gestures and Machine Vision; Java, C++, Assembly). |

SKILLS

Infrastructure & Virtualization

- KVM, ESXi, Hyper-V, BSD Jails | Docker, VMware Workstation, VirtualBox
AWS, Azure, GCP | System Hardening (Debian, Red Hat, SELinux, AppArmor)

Security & Automation

- SIEM, IAM, TLS/x.509, Zero Trust, Network Segmentation
Bash, PowerShell, Python | Jenkins, GitLab CI/CD, IaC Pipelines

Tools & Technologies

- PostgreSQL, Redis, Jenkins | Active Directory, LDAP, Microsoft 365
Cisco IOS, OPNSense, Nmap, Wireshark | VeraCrypt

Programming & Reverse Engineering

- C, C++, Python, Assembly | Java, JavaScript, Ruby
IDA Pro, Ghidra, Radare2 | Exploit Dev, Debugging, Disassembly

COMMUNITY INVOLVEMENT

09.2024 GrrCON, Event Volunteer

Grand Rapids, MI

Supported conference operations over three days, assisting with attendee logistics and on-site coordination to support the security community.