JUSTIN T. KNOX, BSc, CISSP
+1 (843) 534–6040 | justin.knox@posteo.de
https://linkedin.com/in/justintknox | https://jknoxdev.github.io | https://github.com/jknoxdev

SUMMARY:

• L3 Networking, Systems & Cyber Security Engineer with 20 years of experience in the tech industry.
• 10+ years of professional experience in automation, support and development.
• Demonstrated leadership, problem-solving and adaptability with expertise in mentoring, training and project delivery.

EXPERIENCE:

Senior IT/OT Infrastructure Administrator, ICS/OT Cyber Security (LIII) Sep 2023 - Present
Great Lakes Water Authority, Operational Technology Cyber / Information Systems Security | Direct-Hire | Onsite to eventual 20% Remote | Detroit, MI
Developed, implemented and maintained the information, operations and network technologies of the Great Lakes Water Authorities process control network; in accordance with the guidelines published within the NIST's Cybersecurity Framework 2.0 and 800-153 documents.
• Piloted the internal IAM system for organizational internal use, increasing password entropy complexity within the organization by 8 %.
• Implemented TLS 1.3 authentication for an increased usage of authenticated encrypted sessions by over 43%.
• Designed, developed and deployed the internal Internet Protocol Address Management (IPAM) and network design platform on PostgreSQL, Redis and Jenkins platform-based technologies.
• Built, deployed and tuned an additional internal SIEM to increase network visibility by 60%; with increased visibility into network related events by 2 orders of magnitude.
• Conducted and implemented an internal organizational Data Security program, in line with full CSF 2.0 adherence.
• Developed and implemented malware analysis, categorization and archival systems.
Skills: JSON · ReST · JavaScript · PowerShell · NMap · SIEM · Suricata · Splunk · ElasticSearch · Snort · Salt · Puppet · Chef · EPO · EDR · EDS · DLP · CMBD · IPAM · Metasploit ·Cisco ISE · Cisco DNA · FortiNAC · FortiGate · Windows AD / Active Directory · LDAP · x509 · TLS 1.3 · DNS · DNP3 · Modbus · NIST 800-153 · CSF 2.0 · Wireshark · tcpdump · nc · nmap · IAM · Nessus · Purdue Model · SCADA

Systems Engineer June 2023 – Sep 2023
Corewell Health, Critical Environment Engineering (CEE) | Contract, MaTech Resources | Onsite to eventual %20 Remote | Grand Rapids, MI
Collaborated with the cross-functional agile train to deploy, provision, and maintain the companies existing and future infrastructure across OSI L1-4.
• Doubled the production compute infrastructure within a 40% faster than estimated delivery time through providing experienced deployment methods using industry best practices.
• Decreased CEE related incidents by 4% through complete audit and documentation overhaul for the East MI region (in progress).
Skills: SQL· JavaScript · GitHub· Python · PowerShell · Bash · Splunk · SCADA

Sr. Network Engineer March 2023 – June 2023
jPeg Design | Research & Development, Deployment, Support & Maintenance| Direct-Hire |100% Onsite | Dundee, MI
Worked in a 3-person team to design, deploy and maintain small to medium business infrastructure.
• Developed the company's first inventory, customer, client and installation databases, effectively eliminating 15 hours / week / user for prior data entry.
• Developed in-house automation software, including password management and deployment monitoring software.
Skills: PostgreSQL · Python · GitHub · Azure PostgreSQL · AWS · GCVE · PowerShell · Bash · MoIP· Cisco CLI

Freelance Technical Consultant, CTO December 2021 – March 2023

Alchemy Computing, Dumptd | Research & Development, Systems Architecture | Direct-Hire | 100% Remote | Washington DC

Developed and implemented features, coordinating with engineering teams for the prototyping of front end and back-end systems in the creation and deployment of company infrastructure. Primary clients were in the startup space.

Skills: Laravel· Ruby· Ruby-on-Rails· PHP· TomTom API· Google Maps API· Ansible· Docker· Python · GitHub · RedHat KVM· Docker· GCVE · Active Directory· Windows Server 2016· MoIP· VoIP· Cisco CLI· Juniper· pfSense · PlatformIO · JSON · HTML · MySQL· PostgreSQL · OpenBSD · Iptables · Palo Alto Firewalls · RFID · QR-Code Programming

Senior Infrastructure Operations Engineer (LII), GCVE Tech Lead (LIII) December 2018 – December 2021

Google | Engineering Field Services, Server, Network & Hardware Operations Teams | Direct-Hire, Tech-level 3 | Reston, VA

Worked in the global EFS team covering all architectures for the entirety of the Google production fleet. Collaborated with a 12-member team to lead projects and teams to deploy, maintain and configure the production infrastructure from Layers 1 – 4 of the OSI model.

• Provided zero loss to five-9 SLO and SLA during the 400% increase to production load of the Covid-19 outbreak with an 80% reduction in staff.

• Saved the company an estimated $450k in lost compute time to isolate an issue occurring on the power line which took 8 months to gather the data for conclusive enough evidence to change the design.

• Led the project team which deployed 1/3 of the GCVE infrastructure in which we were able to complete the project 75% ahead of schedule. All contractors on the team were converted to full time.

• Built and deployed globally distributable internal systems monitoring, configuring and reporting software to effectively eliminate 80% of my original job functions.

• Hosted and developed internal “lunch & learns” covering Emacs, Linux and systems internals w/ 12-20 people in recurrent attendance.

• Received 19 Peer Bonuses and 2 Challenge Awards for Hurricane and Pandemic Support

Skills: SQL· GSQL· Kubernetes · CI/CD· HTML· JavaScript· CSS· Bash· C++

Network Operations Technician July 2017 – December 2018

Switch LTD | Network Operations | Contract to Hire | 100% On-site | Las Vegas, NV

Coordinated with engineering teams to provide infrastructure support.

• Implemented custom programmed outlook filters combined with email lexical analysis to autogenerate tickets based on customer emails saving approximately 65% of time spent answering emails.

Skills: AutoHotkey · BGP · PowerShell · Splunk

Systems Administrator IV October 2016 – June 2017

Pinnacle Community Services | Information Technology | Direct-Hire | 100% On-site | Las Vegas, NV

Worked in a marketing automation platform organization, assisting businesses of various sizes. Collaborated with a 1,200-person team to improve security and comply with SOC 2 and PCI-DSS. Led projects to strengthen security processes and promote best practices.

• Developed internal file-share-system and converted over to bring organization into HIPAA compliance.

• Created Porteus system images to access in-house customer care system from Windows XP machines for approximately 30 remote sites.

• Secured the companies trunks using IPsec over GRE on Cisco and Avaya infrastructure.

• Saved the company approximately $80k from unneeded legal hours through conducting an in-house investigation using the Sleuth digital forensics toolkit to procure documents required for discovery.

Skills: Cisco· Avaya· Windows Server 2012· Active Directory· Samba· Kerberos· Porteus Linux· Java· PowerShell · BSD

Technical Specialist II November 2013 – April 2015

Scientific Games | Technical Documentation and Training | Direct-Hire | 100% On-site | Las Vegas, NV
practices.

• Brought travel expenditures down by 95% through creating a digital library of in-house training videos through the Casino Laboratory that our team also created.

• Saved approx. 650 hours / week in labor through consolidating the Geographic Dependent Jurisdiction codes technicians were sourcing in to a single database.

Skills: Microsoft SharePoint· Arch Linux· PHPFM· Memcached· NGINX · Apache· WordPress · Jekyll· Markdown · Yammer

Freelance Technical Consultant September 2009 – November 2013

Alchemy Computing | Information Technology | Las Vegas, NV
practices.

• Focused specialties included in-home PC Repair, small website development, electronics prototyping.

Skills: C++ · OpenCV · Java · Processing · NodeJS · Bluetooth Protocol · RTSP · MIDI · ClamAV · Malware Removal · Digital Forensics · Data Recovery

Network Event Management Technician III May 2008 – September 2009

British Telecom| Converged Services Management Center| Contract-to-Hire | 100% On-site | El Segundo CA
Assisted with the internal acquisition of Infonet's global NOC to the UK's infrastructure.

• Kept the UK's network functional through the 2008 Olympic games through acquiring total coverage over the management platform for OSI L1-3 over a Cisco, Juniper, Alcatel-Lucent, Ciena mixed platform.

Skills: MPLS, EIGRP, IGRP, SDH, PDH, ATM Frame-Relay, TCP/IP V4/V6, SIP, ARP, CDP, CARP, EIGRP, OSPF, BGP, VTP, EtherChannel, 802.1Q trunking, QoS, Multicast, 802.11a/b/g/n/ac, IPsec, LDAP, RADIUS/TACACS+, SNMP, NTP, VRF and HTTP/HTTPS

Junior Electronics Engineer June 2006 – November 2007

Synetcom Digital | Research and Development | Direct-Hire | 100% On-site | El Segundo, CA
Worked in the engineering team developing industrial SCADA radios for monitoring digital IO, 4-20ma sensor loops, PWM, and industrial video applications.

• Provided increased customer acquisition through developing the GUI for the PLC system's first user control panel.

• Prevented external theft of IP through securing the internal LAN communications prior to one particular vendor visit.

Skills: digital IO · Industrial Automation · 4-20ma sensor loops · PWM· Allen Bradley · PLCs · PIC Programming · BASIC Stamp Development · Propeller Chip· FHSS · Antenna Design and Implementation · EagleCAD · EWB · National Instruments · Oscilloscope · Function Generator · Traffic Generators · Standard Laboratory Equipment · Spectrum Analyzer · Embedded Linux · Windows CE · C++ · Ladder Logic

Tutor and Laboratory Technician March 2004 - June 2006

DeVry University | Network Laboratory | Direct-Hire | 100% On-site | Long Beach, CA
Tutored students in the network security and advanced micro peripheral courses. Focused specialties included:

• Network Design, Engineering & Architecture
• Cisco CLI commands, interfacing and scripting.
• Implementing network configurations with Java
• Network Packet analysis

Skills: C++ · Java · Wireshark · Cisco · Novell · Windows 2000 Networking · RedHat Linux · Gentoo · TCP/IP Packet Optimization

EDUCATION:

University of Tennessee, Knoxville — Knoxville, TN
M.S.C.S. Data Science and Intelligent Systems (IN PROGRESS) — PROJECTED December 2025
Thesis: (to be determined)

DeVry University, Long Beach — Long Beach, CA
B.Sc. Full-Time Program, Honors Graduate, GPA: 3.6 — March 2008
• Successfully completed thesis project "Fingertip Effects". A machine vision project which tracked LEDs worn on a user's hands (in a glove) to generate effects and change the output of music. The Project used a serial link processed by the Motorola HCS12 and a custom protocol I developed to interface with the Analog Device Blackfin DSP which then processed the effects on the music. We were awarded Best Senior Project for the year.
• Associated Student Body President, Spring 2005 – Fall 2005, Spring 2006-Fall 2007

CERTIFICATIONS/PUBLICATIONS/PROFESSIONAL ASSOCIATIONS:

• CISSP / Certified Information Systems Security Professional
International Information System Security Certification Consortium, ISC2, Active as of: March 2024

• SEC+ / Security+
Computing Technology Industry Association, CompTIA, Active as of: December 2023

SKILLS:

• Languages: C, C++, Java, SQL, BASH, LaTeX, YACC, YAML, XML, HTML, CSS, JavaScript, Ruby, Python, Assembly
• Cloud / Server / HyperVisor Operating Systems: Windows 10, Windows 2016, RHEL 7, Linux (VMWare), ESXi, OpenBSD, FreeBSD, NetBSD, Docker, XCP-NG, EVE-NG, VirtualBox
• Windows: Sysinternals, PowerShell, Windows Subsystem for Linux, WMIC, Firewall, and Registry
• Virtualization: ESXi, VMware, VirtualBox, Docker, AWS EC2

PROJECTS:

"Homelab" - FOSS Home Computing
https://sites.google.com/view/justinsdevlab/home
Description:
Fully self-hosted search, DNS, firewall, remote access, file storage, cryptocurrency mining and blockchain hosting.
Technologies used:
SearxNG, dnsmasq, Cisco 1841, Palo-Alto PA-500, OpenVPN, IPSEC, GRE, BGP (dn42), FreeNAS, NFS, Monero, Dash, Litecoin, Ethereum, Bitcoin (miners and full-nodes)

"Cyboard" - Longboard Security System and Datalogger
Description:
Raspberry Pi based "Smart skateboard", with on-device weather detection, key fob to "lock" the board, motion and location detection for "ride-data".
Technologies used:
Python, SQLLite, GPS PA1616S, Raspbian, NeoPixel LED, Remote Control Encoder PT2262, SHT30 Sensor, ADXL343 - Triple-Axis Accelerometer

VOLUNTEER/LANGUAGES/AWARDS:

- Awards: Best Senior Project 2008.
- Social Languages: (Almost) Conversational in Spanish, Studied Portuguese in Brazil, Serbian in Serbia