Justin Knox, B.Sc., CC

2232 S Main St. #292, Ann Arbor MI, 48103 | M: 313.466.2808

justin.knox@posteo.de | linkedin.com/in/justintknox | @github.com/jknoxdev
@gitlab.com/n1ghtcr3w | @techbiotic:matrix.org

Objective: Security Operations Engineer

Experience:

University of Tennessee, Knoxville | Graduate Student

Studying for Masters of Science in Computer Science | Online, Ann Arbor, MI | Dec 2022 – Present

- Specialization is in Data Science & Intelligent Systems; with Dual-Major in Software Engineering.

Alchemy Computing | Freelance Technical Consultant

Fullstack Development, Systems Architecture & Design | Ann Arbor, MI | Dec 2021 – Present

- Services include, small business infrastructure design, development & deployment, full-stack development, wireless network design and server disaster recovery.
- Notable clients are primarily in the legal, entertainment and construction industries.

Google | Operations Engineer II / DT3

Global & 3rd Party Datacenter, Engineering Field Services, Hardware, Network & Server Operations | Charleston, SC; Reston, VA | Dec 2018 – Dec 2021

- Deployed, maintained and configured the Cisco ISRs and Juniper L3&L2 switches on the production network to the Google Cloud GCVE east coast deployment. The project was completed 60% faster than was scheduled.
- Developed internal BASH, KSH, ZSH Shell scripting automation, dashboards and tools to administer and apply technical solutions to deployment, maintenance and production systems. Languages included Python, Ruby, JavaScript/ECMAScript, SQL,HTML, and CSS on the internal CI/CD “Git like” CVS.
- Provisioned, maintained and managed biometric, RFID, and physical building access systems and user credentials to gain access.
- Worked closely with Security Operations and Network Deployment teams to provide physical penetration testing on production infrastructure protection devices and ensure integrity of the units.
- Ensured and maintained the (server internal) proprietary cryptographic electronic protection devices and provided root cause analysis for faults in the production servers.
- Provided engineering field services of deployment, configuration and troubleshooting of Google servers, network and infrastructure devices.

- Deployed, maintained and configured the internal rack security units as well as external physical perimeter protection devices.
- Received 19 Peer Bonuses, and 2 Awards for Hurricane & Pandemic Support.

Switch LTD | Datacenter Technician

Network Operations | Las Vegas, Nevada | July 2017 – Dec 2018

- Deployed customer network configurations from schematic to configuration, utilizing a wide variety of industry vendors including Cisco, Juniper, Cienna, Palo-Alto, Dell, HP, Checkmate, Alcatel-Lucent as well as other proprietary equipment.
- Provided network incident detection in the internal Network Operations Center and issue escalation, for outages on customer nodes as well as production upstream links.
- Coordinated with Engineering teams from over 2,300 customer deployments to provide regional technical support issues on customer provided infrastructure ranging on deployments that ranged from 1RU, to multi-campus / LAN and multi-sector-wide / WAN deployments.
- Ensured perimeter security and conducted routine production infrastructure security audits in compliance with customer provided ISO specifications.

Pinnacle Community Services | IT Support Technician IV

Information Technology | Las Vegas, Nevada | Oct 2016 – June 2017

- Designed and implemented the internal communications network for the regional office back to the headquarters using IPSEC over GRE on Cisco 2800 series ISRs, and 3600 series layer 2 switches.
- Implemented, secured and converted the VOIP infrastructure to its own internal VLAN.
- Provided systems administration, network design, deployment and support for the Nevada region covering 30 remote locations and three office campuses; in a mixed Windows Server 2016, RedHat, OpenSuse, FreeBSD and Ubuntu environment.
- Designed, built and migrated the company back-end infrastructure over to HIPAA compliant, open source and license free solutions.• Implemented strategy to acquire ISO 27001 compliance for the internal datacenter.
- Conducted forensic investigations to procure data for human resource and legal departments utilizing Autopsy, the Sleuth toolkit, PhotoRec and self-developed Log analysis software.
- Modified and secured the Active Directory Group Policy Objects of the production network to properly reflect and align with organizational restructuring.
- Converted the existing field deployments, developed the internal Linux images and deployed over 30 locations across the Nevada region.
- Hardened the file server and converted the internal deployment to comply with TLS 1.3

- Created and migrated the data storage servers to fully encrypted internal storage at rest and in transit.
- Created the secondary backup file servers and using best practices; security hardened the BSD platform.

Scientific Games | Technical Specialist II

Technical Training & Documentation | Las Vegas, Nevada | Nov 2013 – April 2015

- Designed and built the mem-cached Arch Linux prototype server infrastructure to distribute the in-house training videos out via the company WAN.
- Using security best practices, securely hardened the production instances of the Arch Linux kernels; and implemented the IP tables firewalls for each of the units.
- Interfaced with Hardware & Software Engineering teams to develop internal training to distribute to ~680 technicians globally on a monthly release cycle.
- Designed, developed and deployed the companies first Casino training laboratory. This mirrored the in-field deployment for the entire product line of gaming machines and networks.
- Wrote, filmed, edited and distributed training content using video production methodology to integrate into videos for distribution using Adobe Premiere, AfterEffects in the five phase production lifecycle.
- Created training scenarios to match and emulate the field failure conditions to assist in the training of new technicians. Conditions matched that of all possible conditions seen in the field.
- Managed and created the company's internal training database utilizing SQL on a MySQL deployment; and implemented it into its eventual migration to the production SharePoint servers.

Alchemy Computing | Freelance Technical Consultant

Web Development, Computer Repair, Electronics Prototyping | Los Angeles, CA | Sept 2009 – Nov 2013

- Services included, small business desktop and infrastructure support, web development and design, electronics product prototyping development, wireless penetration testing, data recovery, forensic analysis, wireless network design and server disaster recovery.
- Notable clients were primarily in the legal, entertainment and cosmetic industries.

British Telecom | Network Event Management Technician III

Global Operations Tier 3, Converged Services Management Center | El Segundo, California | May 2008 – Sept 2009

- Provided Tier 3 support, including the provisioning, maintenance and performance monitoring of BT-Infonet's internet backbone; in a cross-platform; mixed vendor environment; platforms included Cisco, Alcatel Lucent, Juniper & Cienna based equipment.

- Protocols included: MPLS, EIGRP, IGRP, Frame-Relay, TCP/IP V4/V6, SIP, ARP, CDP, 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.
- Designed, developed and implemented a computer vision application utilizing the OpenCV API to notify technicians of network alarm status.
- Advised and implemented security best practices when creating the workstation access system images to match the required software to manage the Converged Services Management Center at the Global Network Operations Center.
- Gathered and analyzed network traffic telemetry data and prepare documentation for engineering team analysis.
- Gathered and developed the internal documentation website for incident management reporting.

Synetcom Digital | Junior Electronics Engineer

Torrance, California | June 2006 – Nov 2007

- Designed and converted existing customer networks to support fail over resistant mesh network topology utilizing FHSS (frequency hopping spread spectrum) radios.
- Conducted Wireshark traffic and packet analysis to help secure and harden SCADA radio networks in point-to-point, star, bus and wireless mesh topologies.
- Developed and implemented software utilizing the embedded System on Chip encryption modules with AES256 to secure video over radio communications.
- Conducted Kismet, Spectrum analyzers and custom built software to conduct wireless penetration testing to ensure communication security.
- Developed and implemented IPSec on the Active Directory LAN intranet and secured it in a mixed windows Linux development environment.
- Worked in the engineering team developing industrial SCADA radios for monitoring digital IO, 4-20ma sensor loops, PWM, and industrial video applications.
- Designed, conducted and implemented quality assurance and field simulation testing for complete product range.
- Created laboratory experiments to emulate exhibited field errors and develop for more solutions to solve them.
- Researched and integrated emerging technologies into new products for field deployment.

DeVry University | Academic Tutor

Office of Academic Support and Instruction Services, Advanced Development Laboratory, Network Laboratory, Computer Laboratory, Electronics Laboratory | Long Beach, California | Mar 2004 – June 2006

- Assisted students with usage of laboratory equipment for assignments and experimentation.

- Tutored students in the office of academic support and instructional services,advanced development laboratory, as the resident Teachers Assistant in the network security and advanced micro peripheral courses.
- Focused specialties included:
- Password cracking
- Wireless network penetration testing
- WEP network cracking traffic
- Packet analysis
- Digital forensic techniques
- Data reconstruction from hard drives (TestDisk, PhotoRec)
- Digital forensics avoidance techniques
- Nmap
- Social engineering techniques
- Reconnaissance

Technical Skills & Security Tools:

Vulnerability Assessment Tools:

Nmap, Net Stumbler, Netcat, Kismet, Wireshark, Kali Linux, Pentoo Linux

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

Applications:

Office, Sharepoint, Adobe Premiere, Adobe After Effects, Adobe Photoshop, Adobe Illustrator, MATLab, Slicer (3D Printing)

Databases:

PostreSQL, MS SQL Server 2008, MS Access, MySQL

Education:

Graduate Student, Master of Science in Computer Science

University of Tennessee, Knoxville, Dec 2022 - Present

Web Development Full Stack Bootcamp

LeWagon, Rio de Janeiro, Brazil, June 2021 - Sep 2021

Bachelor of Science, Computer Engineering Technology

DeVry University, Long Beach, California, Oct 2003 – March 2008 GPA: 3.58, Summa Cum Laude, Academic Honors: Dean’s List, 2003 – 2007

Certificates:

(ISC)² Certified in Cybersecurity / CC

International Information System Security Certification Consortium (ISC)² Active as of: September 2022