Robin Reel

Springfield, MO (open to relocation or remote) | robin@dreamstation.systems | (417) 414-0502 | https://dreamstation.systems/professional/

Security-minded full-stack IT and systems generalist. Seeking full-time employment beginning May 2027.

Education

Bachelor of Science in Information Technology, IT Infrastructure Track — *Missouri State University*, *Springfield*, *MO* *Expected May 2027*

Certifications

CompTIA A+, CompTIA Network+, CompTIA Security+ *All earned 2026*

Technical Skills

	Proficient	Familiar
Operating systems:	Linux (server and desktop), Windows desktop	Windows Server
Infrastructure and tools:	SonicWall, email hosting, DNS configuration, Wazuh	VMware ESXi, Samba, Nmap, Wireshark, Git, systemd
Endpoint management:		Microsoft Intune, Entra ID (Azure AD)
Programming:	C, Bash	Perl, SQL, Python, JavaScript/TypeScript, Go

Work Experience

IT Specialist *(August 2026 – Present)* · **IT Intern** *(April 2026 – August 2026)* — Health Hub Clinic & Health Guardian Imaging

- **Found and escalated a PHI-exposing authentication bypass vulnerability in the in-house EMR; verified developers' remediation**
- **Discovered an unauthenticated endpoint allowing attackers to HTTP PATCH patient charts, including medications and allergies; verified remediation**
- Replaced near-EoS Windows Server 2016 infrastructure (file server and AD DCs) with Samba on Debian Linux, saving ≥$3,000 in upgrade costs
- Configured and deployed Wazuh SIEM, with agents on office servers, ~20 workstations, and the PACS gateway
- Found three vulnerabilities in other in-house software (stored XSS via poorly sanitized UGC, two instances of broken access control exposing private messages); fixed two and escalated one to developers, verified remediation
- Configured Intune compliance baselines and Entra ID Conditional Access policies supporting HIPAA compliance for Windows, Office, and Teams
- Documented the network environment when no documentation existed by using Nmap, analyzing SonicWall configuration, and physical tracing
  - Discovered and fixed security issues during this process (SMB signing disabled, EoS software running, unencrypted DICOM on the general office LAN)
- Migrated aging PACS gateway to a virtualized environment, resolving frequent downtime after original hardware began failing
- Discovered long-standing unenforced DMARC and broken SPF on one domain; demoed email spoofing and then remediated
- Conducted authorized phishing simulation; crafted custom replica Google login and document sharing email; communicated results to leadership
- Replaced a double-NATing wireless router with managed APs; migrated end-of-support SonicWall TZ600 to a modern TZ670
- Restored server access in 2 hours after storm damage to a jumpbox; diagnosed electrical pitting on a RAID controller pin and shimmed the connection
- Migrated an off-site VPN-connected NAS to the on-site LAN and reintegrated it with SonicWall, Windows clients, and imaging system clients

Open-source Contributions and Security Research

Manifold Markets — **Discovered and responsibly disclosed a double-spending bug in limit orders and was awarded a bug bounty**

OpenEMR — **Independently discovered and reported an integrity issue; credited as Finder on GHSA; awaiting public disclosure and CVE assignment**

Arch User Repository — Maintainer for seven packages; writing build scripts with signature verification to distribute software to Arch Linux users via Git

Upstream Contributions — Nine pull requests merged into existing projects; contributed to Toki Pona localizations for Firefox

Projects

Homelab: dreamstation.systems — Public-facing server hosting NTP, email, HTTP, Gopher, Gemini, and several other protocols

dreamstation.systems hosts a high-speed NTP and NTS server participating in pool.ntp.org that serves **>500 million NTP requests per day**, a personal email server with SPF, DKIM, DMARC, MTA-STS, and TLS-RPT correctly configured, an obfs4 Tor bridge, and a VPN that my home DMZ connects to.

Homelab: home network — Configured a segmented home network using VLANs; using a Wazuh SIEM instance to gather logs and flag anomalous traffic

- Automated parsing and summarization of unsupported log sources using Perl scripts, Bash scripts, and local LLMs (Qwen models)

!~ATH — Esoteric programming language (https://github.com/robinpie/ath)

- Designed and developed a concurrent programming language where all control flow waits for entity death; supports networking, I/O, and a C FFI
- Wrote a self-hosting transpiler to C89 via continuation-passing style transform, including >500 unit tests; supports Linux, Windows, and WASM
- Simulated QUIC transport behavior in !~ATH for a networking class project, with congestion control, loss detection, and retransmission across 4 streams

Xcaca — X Window System server in ASCII art (https://github.com/robinpie/xcaca)

- Implemented an X server built on Kdrive that renders graphical output as ASCII art in a tty; synthesized evdev scancodes from libcaca character events

ilo toki nasa — Trained an 11M-parameter smolGPT-style LLM decoder on the Toki Pona language; cleaned training corpus through rule-based filtering

OpenGET — Old School RuneScape Grand Exchange market analysis tool (https://grandexchange.dreamstation.systems)

- Built a market analysis tool and price tracker for Old School RuneScape's in-game economy using a Go backend and a SQLite database
- Ingests data from a public API into a tiered archive with a 5-year backfill; dual-pool WAL SQLite with nightly rollup, prune, and compaction
- Built an accountless, cookie-based identity model (128-bit tokens encoded in Crockford Base32); only SHA-256 token hashes are stored server-side
- Developed a novel shared document model; make a change in one place and have it rendered into HTML, gemtext, Gopher maps, and plaintext