Jefferson S. Lawrence

Merrimack, NH | JSLawrence@comcast.net | LinkedIn | status.jslawrence.org

PROFESSIONAL SUMMARY

- Cybersecurity and systems professional with 20+ years supporting large-scale financial services environments, with deep experience in incident investigation, enterprise Linux administration, and disaster recovery operations.
- Proven ability to drive cross-functional remediation efforts, document processes, and maintain operational integrity across complex, high-availability production environments.
- MS in Cybersecurity (4.0 GPA) and BS in Information Technologies, Magna Cum Laude — with dual concentrations in Networking and Cybersecurity.
- Builds and operates a multi-host security homelab (pfSense, Wazuh SIEM, Prometheus/Grafana, Ansible) with a live, sanitized public status page; practices defensive security on HackTheBox and TryHackMe.

SKILLS

Cybersecurity & Tools: Splunk (SPL), Wazuh SIEM, Prometheus/Grafana, Vaultwarden, defensive security practice via HackTheBox and TryHackMe

Networking: TCP/IP routing, dual-subnet architecture, iptables/NAT, DNS (authoritative and recursive), pfSense, static routing, Cloudflare (DNS, DNSSEC, Workers)

Systems & Scripting: Linux/RHEL, Bash, SQL, Ansible, Docker, AWS

IT Operations: ServiceNow, Jira, Control-M, CommVault, Symantec NetBackup, Legato

Platforms: Windows, AIX, Solaris, Stratus VOS, Linux (multiple distributions), OS/400 (former Technical Specialist); historical experience with IBM Mainframe and DEC Unix

Certifications & Training: TestOut Linux Pro (2017), Udemy

PROFESSIONAL EXPERIENCE

Systems Services & Support Analyst 2021 – Present

Fidelity Image Management Services Group (FIMS) | Merrimack, NH

- Tracks and maintains a portfolio of 13 Disaster Recovery plans, executing recovery operations and rehydration of critical systems as needed — including cloud-based application recovery on AWS.
- Validates system and application functionality following weekly server patching cycles covering up to 15-20 systems per cycle, maintaining production integrity.
- Applies Splunk SPL to investigate user-reported production incidents, identifying root causes and documenting findings to support future triage and reduce recurring issues.
- Tracks and resolves incidents in ServiceNow and Jira, ensuring timely remediation and clear documentation in support of operational accountability.
- Performs Linux (RHEL) administration including file operations, cron scheduling, and process management to maintain stable production operations.
- Developed Bash scripting solutions to automate process cycling via cron, improving operational efficiency.
- Contributing to ongoing enterprise documentation migration from SharePoint and OneNote to Confluence, modernizing the team knowledge base.
- Maintains currency through continuous learning via Udemy and Degreed.

Technical Support Engineer 2018 – 2020

Barracuda Networks | Chelmsford, MA

- Delivered technical support to external subscribers and partners resolving backup and recovery issues across Windows and Linux platforms, ensuring data availability.
- Created and maintained detailed ServiceNow incident records, documenting resolution steps to build a reusable knowledge base for future triage.

Systems Services & Support Analyst 2016 – 2017

Fidelity Brokerage Technology (FBT) Group — Via Tek Systems / Veritude (Contract) | Merrimack, NH

- Participated in ServiceNow platform evaluation, providing operational feedback to support enterprise-wide transition.
- Conducted Splunk log analysis to identify root causes of production processing incidents.
- Coordinated incident response including conference bridge management, stakeholder notification, and post-incident documentation.

Operations & Support Roles (Progressive) 2001 – 2016

Fidelity Investments / JP Morgan Chase Paymentech | Merrimack, NH & Various

- Progressed through tier 1 console operations to systems analyst roles, supporting enterprise backup environments across Solaris, AIX, RHEL, and Windows platforms.
- Served as local CommVault Commcell administrator managing backup operations across 2 Commcells (~1,300 hosts, ~3,000 daily backups) spanning Windows, Unix, and Linux platforms.
- Performed Control-M job scheduling, Stratus VOS operations, and RHEL system analysis to ensure timely production processing.
- Participated in SEC Messaging Restores Analysis Project (Discovery), utilizing CommVault, NetBackup, Legato, and ArcServeIt to satisfy regulatory obligations.
- Served on rotating tier 2 on-call escalation duty, providing off-hours production incident support.

EDUCATION

Master of Science in Cybersecurity

GPA 4.0 | Southern New Hampshire University, Manchester, NH

Bachelor of Science in Information Technologies

Magna Cum Laude, GPA 3.8 | Dual Concentrations: Networking & Cybersecurity | Southern New Hampshire University, Manchester, NH

HOMELAB SECURITY & MONITORING

Self-built, multi-host security lab ("the Nebula"), with a live, sanitized status page at status.jslawrence.org.

- pfSense firewall fronting a routed lab subnet, with firewall logs ingested into the SIEM.
- Wazuh SIEM with five agents across Linux and Windows hosts; least-privilege, read-only service account for dashboard integrations, with alert data kept local to the SIEM host.
- Prometheus and Grafana monitoring across Linux, Windows and pfSense hosts, including smart-plug power metering.
- SSH key-only access enforced on core Linux hosts through Ansible playbooks; credentials held in Ansible Vault and a self-hosted Vaultwarden.
- DNS built on Pi-hole and Unbound for recursive resolution and BIND9 as the authoritative server for the internal zone; DNSSEC, CAA, SPF and DMARC configured on the public domain.
- SITREP: self-hosted threat-awareness dashboard combining CISA KEV, advisories and security news with live SIEM agent and alert status.
- Public status page on Cloudflare Workers, fed by a fail-closed, allow-list exporter that refuses to publish anything resembling an IP address or hostname.