SCOTT ALESSIO

SYSTEMS ENGINEER · INFRASTRUCTURE · NETWORKING · CYBERSECURITY

Paramus, NJ 07652 | (201) 615-0018 | scott42703@gmail.com | linkedin.com/in/scott-alessio-4b1743287

PROFESSIONAL SUMMARY

Engineer with an M.S. in Cyber Security and Privacy, a B.S. in Computer Engineering, and CompTIA Security+, currently supporting a 40,000+ server global data center fleet at Bloomberg. Hands-on across Linux, enterprise networking, server hardware lifecycle, Kubernetes, and Splunk log analysis, backed by graduate work in system security, networking, and cloud computing. Led an 8-person research team to two published papers on network automation and cut emergency staffing costs 12% through automated issue resolution. Open to systems, infrastructure, network, and security engineering roles across New York City and Northern New Jersey.

PROFESSIONAL EXPERIENCE

Data Center Operations Engineer

Bloomberg L.P. | New York, NY and Northern New Jersey | January 2026 – Present

Support the physical and logical lifecycle of a global, high-availability data center fleet of 40,000+ multi-vendor x86 servers, enterprise routers, and switches across paired production sites.

- Investigate infrastructure and hardware faults in Splunk, building searches across system and network logs to isolate root cause and surface recurring failure patterns across the fleet.
- Perform hardware and OS-level troubleshooting across a multi-vendor server fleet, isolating faults at the component, firmware, and network layer to restore availability within service-level targets.
- Troubleshoot pod-to-pod connectivity failures across Kubernetes clusters, tracing east-west traffic paths and inspecting Calico network policy to separate policy denials from node and upstream network faults.
- Execute server and network device installations, migrations, and secure decommissioning under formal change management, maintaining access controls and authoring the runbooks that standardize recurring work.

Information Technology Support Assistant

Ridgewood Country Club | Paramus, NJ | May 2022 – December 2025

Delivered end-to-end IT support for staff endpoints, network infrastructure, and connected systems across a multi-building campus.

- Deployed and hardened an OpenVPN server on a cloud-hosted Linux environment, enabling encrypted remote access for staff and eliminating unsecured remote connection methods.
- Administered user accounts, endpoint configuration, and Microsoft 365 services, handling onboarding, offboarding, and access provisioning.
- Diagnosed network, wireless, and IoT faults across the campus and applied operating system and firmware patches, sustaining uptime while reducing exposure to known vulnerabilities.

Network & AI Research Lead

New Jersey Institute of Technology | Newark, NJ | May 2024 – June 2025

Led an 8-person research team building LLM-driven automation for Cisco network device operations, from prompt design through hardware integration and evaluation.

- Co-authored and published 2 peer-reviewed papers on prompt engineering efficacy for automated network configuration and troubleshooting.
- Engineered a Linux-based, hardware-integrated LLM assistant that automated device management tasks, cutting emergency staffing costs 12% in internal testing.
- Directed evaluation methodology, code review, and publication timelines across the team, analyzing results to raise accuracy and reduce misconfiguration risk.

EDUCATION

Master of Science, Cyber Security and Privacy
New Jersey Institute of Technology | Newark, NJ | May 2025 – August 2026 | GPA: 3.85 / 4.0

Relevant Coursework: Security & Privacy in Computer Systems, Internet & Higher-Layer Protocols, Cloud Computing, Data Mining, Network Security

- Configured and hardened enterprise networks and Cisco devices across Ubuntu, Kali, and Red Hat Linux environments.
- Built and deployed distributed data pipelines on AWS (EC2, S3, EMR) and containerized workloads with Docker.

Bachelor of Science, Computer Engineering
New Jersey Institute of Technology | Newark, NJ | September 2021 – May 2025 | GPA: 3.62 / 4.0

Relevant Coursework: Computer Networks, Cybersecurity, Operating Systems, Computer Architecture & Design, Digital Data Communications, Microprocessor Systems Design

CERTIFICATIONS

CompTIA Security+ (SY0-701)

TECHNICAL SKILLS

Systems & Infrastructure: Data center operations, server lifecycle management, Linux system administration, Windows Server administration, out-of-band management, hardware and firmware troubleshooting, RAID and storage, redundancy and high availability (N+1), backup and disaster recovery, capacity planning, monitoring and alerting, change management, runbooks and technical documentation

Networking: TCP/IP, DNS, DHCP, VLANs, subnetting, routing and switching, OSPF, RIP, NAT, ACLs, firewalls, IDS/IPS, VPN (OpenVPN, IPsec), SSH, 802.11 wireless, structured cabling, network segmentation, port security, packet capture and analysis

Cloud, Containers & Operating Systems: AWS (EC2, S3, EMR, IAM), Docker, Kubernetes, Calico (network policy troubleshooting), container networking, virtualization, distributed data pipelines, Linux (Ubuntu, Red Hat/RHEL, Kali), Windows, Windows Server, macOS, Cisco IOS, Unix

Security: CompTIA Security+, Splunk (SIEM), log analysis, security monitoring, event triage, incident response, threat detection, malware and threat classification, phishing analysis, vulnerability assessment, patch management, endpoint hardening, access control, authentication and authorization, encryption, cryptography, PKI, TLS/SSL, NIST Cybersecurity Framework, MITRE ATT&CK, zero trust principles, defense in depth, least privilege, microsegmentation, risk assessment, security compliance and audit support

Programming, Automation & Tools: Python, Bash, PowerShell, SQL, Java, C, C++, JavaScript, VHDL, MATLAB, RISC-V assembly; Splunk, Wireshark, Nmap, Cisco Packet Tracer, Binary Ninja, MobaXterm, Microsoft 365 Administration, Bloomberg Terminal, Git, ticketing and incident escalation workflows

PROJECTS

Enterprise Network Security Design — Cisco Packet Tracer
Designed and simulated a segmented enterprise network of routers, switches, and hosts; implemented VLAN subnetting and port security to mitigate MAC spoofing and CAM-table flooding, hardening the access layer against Layer 2 attacks.

Secure Serial Data Transmission System — C / RISC-V
Built and tested a serial communication system in C with integrity checking to prevent data corruption in transit; co-designed the supporting circuit network using RISC-V architecture and discrete logic. Presented to a formal technical review panel.