George Neusse

(c) 909-292-5415 | neusse@gmail.com | Seattle, WA

PROFESSIONAL SUMMARY

Senior Splunk Engineer and Architect with deep experience designing, deploying, and optimizing Splunk Enterprise and Splunk Cloud environments across finance, healthcare, and technology sectors. Hands-on expertise includes ITSI, HEC/UF/HF ingestion pipelines, indexer and search head clustering, advanced SPL development, dashboarding, alerting, and KPI design. Proven delivery in AWS environments, Kubernetes observability integrations, and ServiceNow-to-Splunk data architecture. Strong track record in migration programs, performance optimization, disaster recovery design, automation (Python/Bash), and cross-functional technical leadership.

- Public Trust clearance most recently held under IRS contract.

CORE SKILLS

- Splunk Enterprise and Splunk Cloud (7.x, 8.x, 9.x), Splunk ITSI, Enterprise Security
- Indexer/Search Head clustering, HEC/UF/HF ingestion, REST API integrations
- Advanced SPL, dashboards, reports, alerts, KPIs, field extractions, log troubleshooting
- AWS architecture and performance/capacity optimization for Splunk workloads
- Kubernetes observability integration with ITSI entity/metric searches and alerting
- ServiceNow (SNOW) integration for ITAM and asset reporting
- Disaster recovery architecture and cloud/on-prem migration execution
- Automation and tooling with Python and Bash
- Linux administration (RHCT), team mentoring, stakeholder communication

CERTIFICATIONS AND TRAINING

- RedHat Certified Technician (RHCT)
- Certified Biomedical Electronics Technician
- Splunk Training: Developing Splunk Apps, Creating Splunk Knowledge Objects, Advanced Searching and Reporting

PROFESSIONAL EXPERIENCE

Senior Splunk Engineer / ES Admin | VARITE, Inc. (End Client: Adobe)

November 2025 - March 2026 | Remote

- Engaged to stabilize and optimize Splunk Enterprise Security operations supporting security, compliance, and analytics use cases.
- Improved search efficiency across large datasets through SPL optimization, tuning, and workflow redesign.

- Strengthened reliability of Splunk data pipelines and integration/export paths, including near-real-time data flow support.
- Improved indexing, clustering, and correlation search resiliency to increase platform stability.
- Reviewed and rationalized knowledge objects (saved searches, lookups, dashboards) and supported schema-drift monitoring.
- Supported governance controls for access, retention, auditability, and detection lifecycle practices integrated with CI/CD workflows.

Senior Splunk Engineer / IRS Splunk Architect | LynkBlox / IRS

February 2023 - March 2025

- Led IT Asset Management remediation after AWS migration and restored data integrity using Splunk.
- Optimized SPL and reconciliation workflows to resolve migration-related data inconsistencies.
- Enhanced reporting to align with evolving business and compliance requirements.
- Architected a ServiceNow-to-Splunk HEC pipeline to improve ingestion reliability and throughput.
- Integrated Kubernetes monitoring into ITSI with entity and metric searches for KPI/alerting coverage.
- Built asset intelligence reporting from SNOW data to support planning and executive decision-making.

Senior Splunk Engineer | Modis / AmeriHealth

July 2022 - February 2023

- Delivered full on-prem Splunk Enterprise upgrade from v8 to v9 across approximately 90 servers.
- Upgraded Search Head and Indexer cluster members to improve platform reliability, scalability, and security.

Senior Splunk Engineer | TekSystems / 3M

November 2021 - June 2022

- Supported migration of Splunk Enterprise infrastructure to Splunk Cloud with minimal service disruption.
- Engineered AWS dbConnect-to-KVstore data flow to improve data accessibility and operational continuity.

Senior Splunk Engineer | WWT and TSYS

September 2020 - March 2021 | Atlanta, GA

- Managed large clustered Splunk deployments spanning on-prem and AWS environments.
- Built a fully clustered Splunk lab used to train and upskill WWT engineering staff.
- Upgraded Enterprise Security from Splunk 7.3 to 8.1 and advanced ES feature adoption.
- Delivered broad Splunk administration across dashboards, alerts, apps, and REST API-based operations.

Senior Splunk Engineer | Getty Images

November 2019 - May 2020 | Seattle, WA

- Managed an enterprise AWS clustered Splunk environment and migrated on-prem workloads to cloud.
- Integrated SYSLOG-NG/SNMP-NG and Heavy Forwarder add-ons for expanded ingestion coverage.
- Developed Splunk knowledge object exporter/deployer tooling to integrate with GitLab workflows.
- Implemented PagerDuty 429 retry handling and deployed dynamic Splunk DR architecture in AWS.

Splunk Architect | Wipro (Corning and Colgate engagements)

February 2019 - November 2019 | Corning, NY and Piscataway, NJ

- Designed and implemented enterprise Splunk clustered architecture with ITSI.
- Integrated more than 6,600 servers into centralized monitoring for Corning data centers.
- Delivered integrations with AppDynamics, ServiceNow, Oracle monitoring, and backup/storage systems.
- Led multi-data-center and multi-country Splunk/ITSI rollout programs.
- Provided MediaWiki installation, customization, training, and support for knowledge operations.

Splunk Solutions Architect | Ericsson (T-Mobile program)

April 2015 - March 2018 | Seattle, WA

- Built Splunk/Hunk architecture supporting Ericsson-developed billing platforms for T-Mobile.
- Designed custom dashboards and monitoring capabilities for billing operations visibility.
- Implemented SQL integration techniques enabling transparent Splunk time-picker query behavior.
- Delivered Hadoop ingestion monitoring and Splunk disaster recovery clustering.
- Led Hunk with MapR Hadoop deployment for large-scale analytics workloads.

Consulting Systems Lead | UCLA Health

April 2011 - March 2015 | Los Angeles, CA

- Developed Splunk tooling and dashboards for Epic/Cache EHR operations monitoring.
- Served as Cache/Epic DBA and mentored IT teams on platform operations and optimization.
- Implemented MediaWiki customization, training, and support for internal collaboration.
- Built enterprise remote monitoring for AIX and Epic/Cache systems and improved uptime visibility.
- Defined disaster recovery procedures for EHR environments to strengthen business continuity.

Consulting Systems Lead | Cisco

August 2010 - March 2011 | Milpitas, CA

- Developed Splunk-based security threat detection tooling for Apache web server environments.
- Created security status dashboards, enterprise remote monitoring views, and global threat heat maps.
- Improved security operations visibility and response through centralized Splunk analytics.