GRANT HOLMES

grantholmes30@gmail.com ✦ Mobile: 571-206-0657 ✦ Washington, DC

PROFESSIONAL STATEMENT

Grant takes pride in his status as a highly qualified Splunk expert, boasting extensive experience in overseeing deployments and managing Splunk platform operations. With his profound expertise across all facets of Splunk technology management, Grant has successfully designed Splunk deployments and conducted comprehensive operations, encompassing configuration management, data onboarding and analysis, as well as the creation of dashboards and visualizations. Eager to consistently augment his technical prowess, Grant aspires to contribute his valuable skillset to a vibrant and expanding infrastructure and team.

CERTIFICATIONS

CERTIFIED SPLUNK ENTERPRISE ADMINISTRATOR, CERTIFIED SPLUNK POWER USER,
CERTIFIED SPLUNK CORE USER, AWS ASSOCIATE, SECURITY +, RHSCA

PROFESSIONAL EXPERIENCE

CITIBANK – Washington, DC **May 2022 - Present**

SENIOR SPLUNK CONSULTANT

- Data Migration project: Migrated existing Search Head pooling
  Migrated UFs from old hardware to new devices
  Migrated UFs to new deployment server
  Migrated indexers/buckets to new servers
- Customize Splunk Apps and dashboards, build advanced visualizations via XML and HTML, edit configurations as well as maintain reports
- Conducted Splunk upgrades for vulnerability management
- Audited Splunk environment custom TAs configuration props.conf to augment data parsing - performed new line breaking and time format rules to ensure proper parsing
- Carried-out advanced search spl queries to build user content as well as troubleshoot issues within Splunk architecture or ingestion pipeline
- Translate business case analysis into functional requirements
- Debug Splunk and performance-related issues using btool, internal logs and indexes, monitoring console and other network and CLI tools
- Onboard data for numerous application, network, server and SOC teams utilizing various data input ways available in Splunk
- Ongoing data-model/CIM compliance analysis - ensuring to survey data sources to execute field extractions and aliases to map data source to respective data model.
- Highly proficient in using regular expressions (regex) to parse data, conduct field extractions, and query using the rex command
- Create compliance and vulnerability assessment dashboards to analyze configuration and patch vulnerabilities - ensuring to add functionality such as drilldowns, colors, and alerts for the SOC team
- Analyzed historical performance data to identify and correlate incident management performance trends and areas for improvement in IT services and infrastructure.
- Collaborated with IT, DevOps, and E-commerce teams to identify and resolve incidents and problems affecting IT services, using KPI-driven triages views and service deeps dives gained from Splunk ITSI analysis.

T-MOBILE – New York, NY **October 2021 – April 2022**

SPLUNK ARCHITECT

- Designed production-quality Splunk dashboards and created event type definitions
- Developed knowledge objects
- Created automated script to install and configure more than 10,000 forwarders across different OS including Linux, Windows, Solaris and VMWare devices
- Configured and set-up multi-site cluster
- Configured initial setup of CIM to normalize data across varying sources. Normalized 20+ data sources
- Developed and configured data model and pivot tables
- Architected and deployed Search Head Cluster
- Configured LDAP integration with SHC
- Standardized Splunk agent deployment, configuration and maintenance across a variety of UNIX and Windows platforms
- Documented all architectural work on SOPs on Confluence pages

DELOITTE: CYBER & STRATEGIC RISK (VARIOUS CLIENTS) – Hartford, CT **October 2019 – October 2021**

SENIOR SPLUNK ADVISORY & PROJECT SPECIALIST

- Lead the development of operational dashboards providing updates on COVID-19 related risks to mitigate exposure to over 500,000 census field personnel surveying for the 2020 Census Report.
- Lead the automation to develop a continuous monitoring dashboard for COVID-19 risk modeling, forecasting, and vaccination tracking using world modeling.
- Advised the Census Bureau senior leadership on end-user product experience while fulfilling change requests to update their enterprise risk management platform.
- Onboarded data collected from endpoints including Google Workspace, McAfee, Symantec, Arcsight, Oracle, Windows/UNIX syslogs, Attivo, Cylance, RSA, MFA, etc.
- Document technical requirements from customers, create and configure props, transforms, inputs as well as syslog attributions or configure HEC token creation for ingest
- Reviewed the configuration decisions and approve merge changes via GIT integrations
- Developed modules on Splunk search heads that address the latest security scenarios, threats, and regulatory compliance issues using tools such as reports, rules, alerts, dashboards, workflow, visualizations, etc.
- Fully integrated and managed knowledge objects such as lookups, macros, field aliases, data models and data sets to support customer needs
- Developed data correlation rules for Enterprise Security into the Splunk
- Manage Splunk architecture and various components (indexer, forwarders, search head, deployment server, license master)
- Created many of the POC dashboards and data ingestion systems (syslog-ng, nginx, VIP F5 load balancing) for IT operations
- Document best practices, compiled within runbook documentation.
- Build data models using knowledge object types such as lookups, transactions, search and index-time field extractions and calculated fields
- Gathered requirements from client meetings and maintaining records of ingestion work via SharePoint
- Created macros using Rest APIs for various saved searches

WALMART – Springfield, MA **June 2018 – September 2019**

SPLUNK DEVELOPER

- Implement complex deployments of dashboards and reports while working with technical teams to solve
- issues
- Build and implement SIEM reporting to inform and assist clients' incident response teams and security managers
- Troubleshoot and configure UFs on devices, configure database integrations, work with Windows and/or UNIX system administrators to implement configuration changes
- Splunk authentication integrations with Active Directory and Azure
- Integrate new log sources such as VMWare Horizon, Bluecoat, Aruba, Wily, Dynatrace, etc.
- Implement security event analysis and intrusion detection using Enterprise Security in collaboration with Cybersecurity teams (Firewalls, VPNs, VLANs, IDS/IPS Incident response **-** triage, incident analysis, remediation)
- Use Splunk Enterprise REST API that uses HTTP requests to configure and manage Splunk instances, create and run searches.
- Configure AppDynamics integration for application login and application monitoring
- Create and configure various instances of sandboxes.
- Responsible for providing analysis of problems and resolutions/fixes for production issues related to platform within SLA timeframes

ALLSTATE – Northbrook, Illinois **January 2016 – May 2018**

SQL/LINUX ADMINISTRATOR

- Implemented a centralized configuration management system using Ansible, reducing server provisioning time by 60% and ensuring consistent system configurations across a fleet of 100+ Linux servers.
- Optimized system performance by fine-tuning kernel parameters and optimizing disk I/O, resulting in a 30% improvement in overall system responsiveness.
- Led a team in successfully migrating a production environment from on-premises servers to a cloud-based infrastructure, utilizing tools like AWS EC2 and EBS, reducing infrastructure costs by 40%.
- Implemented a robust monitoring solution using tools like Nagios and Zabbix, providing real-time visibility into system health, reducing mean time to resolution (MTTR) by 50%.
- Designed and implemented a disaster recovery plan, including regular backups, off-site replication, and automated failover procedures, ensuring high availability and data integrity in the event of a system failure.
- Developed and maintained a centralized database monitoring system using Nagios, enabling proactive identification and resolution of database issues, reducing downtime by 20%.
- Streamlined database administration tasks by writing shell scripts and automation tools, reducing manual effort by 50% and improving overall efficiency.
- Resolved database performance issues by analyzing and optimizing SQL execution plans, reducing query execution time by 25% and improving overall system response time.
- Implemented advanced database security measures, including encryption of sensitive data at rest and in transit, enhancing data protection and meeting compliance requirements.
- Led a team in the successful migration of critical applications to a Linux-based infrastructure, managing system installation, configuration, and performance tuning, resulting in increased stability and scalability.

COMCAST – Denver, CO **August 2011 – December 2015**

DATA ANALYST/DATABASE ADMINISTRATOR

- Implemented a database replication solution using Oracle Data Guard, ensuring high availability and disaster recovery capabilities, resulting in a 50% reduction in downtime during system failures.
- Manage the oversight of cross-functional teams including data science and operations ensuring that the technical architecture, code quality, and development processes align with business use case deliverables.

- Identified and mitigate technical risks to create dashboards using JSON format for the end users to create actionable insights in their data.
- Coordinated the migration and requirements of legacy customers solutions in AWS production to Google Cloud Platform.
- Developed and executed a comprehensive backup and recovery strategy for MySQL databases, utilizing tools like my SQL dump and implementing a rotating backup schedule, reducing the recovery time by 30% during critical incidents.
- Utilized SQL performance tuning techniques, such as query optimization and index optimization, resulting in a 40% improvement in database query response times and overall system performance.
- Conducted regular security assessments of database systems, identifying and addressing vulnerabilities, and implementing security patches, ensuring compliance with industry standards and regulations.
- Created and managed large datasets to apply comprehensive QA/QC evaluations ensuring all technical requirements were in regulatory compliance
- Developed over 150 variables using ETL frameworks and geo-spatial analytics to create models for strategic data center real estate selection using publicly available and licensed data sources.
- Created business intelligence insights using Tableau to assess automation opportunities for over 100 distribution centers nationwide to better understand the labor market dynamics and the demographics surrounding each proposed real estate location creating actionable insights to invest.
- Collaborated with cross-functional teams to migrate legacy SQL Server databases to PostgreSQL, successfully completing the migration project within the established timeline, resulting in improved scalability and cost savings.

TECHNICAL SKILLS

SPLUNK, TABLEAU, POWER BI, PYTHON, SQL, JUPYTER NOTEBOOKS, DATA ANALYTICS

EDUCATION

Bachelor of Science in Computer Graphics Technology Greensboro, NC
NC A&T State University