**Prudhvi**

**856-484-1614**

**psankati34@gmail.com**

**Summary**:  
  
ExperienceinInformationTechnologyfieldwithstrongexperienceasSoftwareEngineerinSplunkEnterpriseandSplunkCloudfor10+years,andPython,Gitlab,Ansible,AWS.

Dedicatedprofessionalwithprovenperformanceinmanagement,leadership,andcommunication.Detail-orientedinproblem-solvingandplanning.Readytomakeanimmediatecontributiontoyourorganization.

**Technical Skills:**

SplunkEnterpriseSplunkES

Splunk ITSIAnsibleSQL

GCP

SplunkPythonSDKJavaScript

HTML,CSS,XMLSPL

PythonAWS

**Professional Experience:**

**SplunkEngineer Duration 2019-08-23  
T-Mobile**

* Design,engineer,configure,developandcollaborateonthearchitectureandimplementation of an enterprise- scale deployment of Splunk Enterprise. Hands onexperienceinAssistingstakeholdersofSplunkindesigningandmaintainingproduction-qualitydata,dashboardsandvariousapplications.
* Designed, implemented, and maintained complex Splunk architecture to meet organizational data analysis and security requirements.
* Designed and implemented monitoring solutions on Google Cloud Platform using Stackdriver, ensuring the availability and performance of cloud-based applications.
* Integrated GCP logging with Splunk for centralized log management, enabling streamlined analysis and troubleshooting across hybrid cloud environments.
* Successfully led the implementation and configuration of Splunk Enterprise Security (ES)
* Customized and optimized Splunk ES to align with the organization's specific cybersecurity requirements.
* Managed Splunk clusters, including indexers, search heads, and forwarders, ensuring optimal performance and scalability.
* Created and optimized search queries, alerts, and reports to proactively identify and mitigate security threats and operational issues.
* Collaborated with cross-functional teams to integrate various data sources into Splunk, enhancing overall data visibility and analysis.
* Developed complex SPL queries and custom scripts to enhance data analysis capabilities within Splunk.
* Created and maintained advanced dashboards, reports, and alerts using SPL to identify potential security threats.
* Conducted regular data grooming and archiving to maintain efficient Splunk operations and reduce storage costs.
* Implemented role-based access controls (RBAC) and ensured proper user access to sensitive data within Splunk.
* Worked with network and security teams to configure Splunk for threat detection and incident response.
* Collaborated on the development of automated alerting systems, reducing incident response times and improving overall security posture.
* Assisted in the implementation of Splunk's Machine Learning Toolkit (MLTK) for predictive analysis and anomaly detection.
* Ensured compliance with industry standards and best practices for log management, such as CIS and NIST.
* Conducted training sessions for internal teams on observability best practices, Splunk usage, and GCP monitoring tools, fostering a culture of continuous learning and improvement.
* Authored technical documentation and knowledge base articles to share insights and troubleshoot common issues related to observability.
* Maintained up-to-date knowledge of Splunk's latest features and capabilities, integrating new functionalities where appropriate.
* Participated in capacity planning and scalability assessments to accommodate growing data volumes.
* Worked closely with vendors and support teams to troubleshoot and resolve technical issues.
* Optimized Splunk ES performance by fine-tuning searches, data models, and field extractions.
* Improved search efficiency, reducing response times and enhancing overall system performance.
* Streamlined workflows by automating data feeds between Splunk ES and other security solutions.
* Provided training and mentorship to junior team members to enhance their Splunk skills and knowledge.
* Actively participated in on-call rotations to provide 24/7 support for critical systems and incident response.

**SPLUNKENGINEER Duration 2017- 19  
Blue Cross Blue sheild**

**Chicago**

* InstallationandconfigurationofSplunkproductupgradingversionandTestingindifferentenvironmentsinmultipleservers(WindowsandLinux)withautomation.
* Developed and maintained intricate SPL queries and scripts to enhance data analysis capabilities within Splunk.
* Created custom dashboards and reports using SPL, providing real-time visibility into security events and potential threats.
* Administered and optimized Splunk clusters, including indexers, search heads, and forwarders, ensuring scalability and high availability.
* Created, fine-tuned, and optimized search queries, alerts, and reports, leading to proactive threat detection and faster incident response.
* Conducted in-depth analysis of system logs to identify and address cybersecurity exposure points, ensuring compliance with healthcare data security standards.
* Implemented proactive measures to mitigate vulnerabilities and enhance overall security in alignment with healthcare regulatory requirements.
* Successfully integrated Splunk ES with healthcare-specific security tools, such as [mention specific tools], for comprehensive threat intelligence and correlation.
* Streamlined workflows by automating data feeds between Splunk ES and other healthcare security solutions.
* Contributed to the development and automation of alerting systems, reducing incident response times and strengthening security.
* Assisted in implementing Splunk's Machine Learning Toolkit (MLTK) for predictive analysis and anomaly detection.
* Ensured compliance with industry standards, such as CIS and NIST, to maintain the highest standards of log management and security.
* Conducted routine performance tuning and configuration optimization to improve Splunk's efficiency and reduce operational costs.
* Developed and implemented a comprehensive observability strategy for IT systems, leveraging Splunk and GCP services.
* Defined key performance indicators (KPIs) and established monitoring best practices to enhance system reliability and performance.
* Actively documented configurations and shared knowledge within the team, enhancing overall productivity.
* Stayed updated on the latest Splunk features and capabilities and integrated them to improve the company's operations.
* Conducted tailored training sessions for the Blue Cross Blue Shield cybersecurity team on best practices in using Splunk ES and writing effective SPL code.
* Facilitated knowledge sharing sessions to ensure the team stays abreast of the latest cybersecurity trends and methodologies.
* Played a crucial role in developing and maintaining disaster recovery and business continuity plans for Splunk systems.
* Provided training and guidance to junior team members, helping them improve their Splunk skills and knowledge.
* Participated in 24/7 on-call rotations to provide critical system support and quick incident response.

Optimized Splunk ES performance by fine-tuning searches, data models, and field extractions, addressing the specific challenges of healthcare data volumes.

Improved search efficiency, reducing response times and enhancing overall system performance in a healthcare context.

**SPLUNKENGINEER Duration -2016-2017  
Wells fargo, NC**

* WorkedwithuserrequestednewdataonboardingittoSplunkandconfiguredthetypeoflogsingested.
* Spearheaded the implementation and configuration of Splunk infrastructure, improving log management and real-time data analysis capabilities for Cummins.
* Developed custom Splunk applications and dashboards, tailoring them to monitor network and system performance, log data, and security events.
* Administered and maintained Splunk clusters, including indexers, search heads, and forwarders, ensuring optimal performance and reliability.
* Created and fine-tuned search queries, alerts, and reports to proactively detect security threats and streamline incident response.
* Collaborated closely with various teams to onboard and integrate a wide range of data sources into Splunk, enhancing overall data visibility and analysis.
* Managed data ingestion and parsing processes, ensuring accurate collection and indexing of logs from multiple sources.
* Implemented role-based access controls (RBAC) within Splunk to enforce data access permissions and protect sensitive information.
* Worked in tandem with network and security teams to configure Splunk for real-time threat detection and incident response.
* Contributed to the development of automated alerting systems, leading to reduced incident response times and enhanced security measures.
* Assisted in deploying and configuring Splunk's Machine Learning Toolkit (MLTK) to enable predictive analysis and anomaly detection.
* Maintained compliance with industry standards, such as CIS and NIST, ensuring best practices in log management and security.
* Regularly fine-tuned Splunk configurations to optimize system performance, reduce operational costs, and enhance efficiency.
* Documented configurations and shared knowledge within the team, facilitating improved collaboration and productivity.
* Stayed updated on the latest Splunk features and capabilities, integrating them into the environment to enhance operations.
* Played a key role in capacity planning assessments to accommodate growing data volumes and ensure system scalability.
* Collaborated with vendors and support teams to troubleshoot and resolve technical issues, ensuring system stability.
* Contributed to the development and maintenance of disaster recovery and business continuity plans for Splunk systems.
* Provided training and mentorship to junior team members, fostering their growth and expertise in Splunk technology.
* Participated in on-call rotations, offering 24/7 support for critical systems and swift incident response.
* Actively suggested and implemented efficiency improvements in the Splunk environment, contributing to ongoing enhancements.

**LINUXADMIN 2012-12-2015-05  
GGK technologies,Hyderabad,India**

* OverseeITinfrastructureandrespondtourgenttechnicalissues.
* Successfully managed and maintained Linux server environments to ensure smooth operations and high availability.
* Configured and administered various Linux distributions, including CentOS, Ubuntu, and Red Hat, to meet the organization's needs.
* Performed routine system updates, patch management, and security hardening to protect against vulnerabilities and enhance system reliability.
* Implemented and managed user accounts, permissions, and access controls to safeguard sensitive data and enforce security policies.
* Effectively monitored system performance and utilized performance tuning techniques to optimize resource usage and application responsiveness.
* Troubleshot and resolved system issues, including hardware failures, application errors, and network connectivity problems, minimizing downtime.
* Installed, configured, and maintained web servers, such as Apache and Nginx, to host websites and web applications.
* Collaborated with the development team to deploy applications and databases on Linux servers, ensuring seamless integration.
* Utilized shell scripting and automation tools to streamline repetitive administrative tasks and enhance overall efficiency.
* Managed backup and recovery processes to protect critical data, implementing automated backup schedules and recovery strategies.
* Set up and maintained network services, including DNS, DHCP, and LDAP, to support a reliable and secure network infrastructure.
* Administered virtualization platforms, such as VMware and KVM, to create and manage virtual machines for various purposes.
* Contributed to capacity planning and resource allocation to accommodate growth and changing infrastructure requirements.
* Ensured compliance with industry standards and company policies, implementing security best practices and access controls.
* Maintained thorough documentation of system configurations, procedures, and troubleshooting guides for internal use.
* Assisted with the planning and execution of system upgrades and migrations to improve system performance and reliability.
* Conducted routine system audits and vulnerability assessments to identify and rectify security weaknesses.
* Worked with hardware vendors and support teams to address hardware issues and maintenance requirements.
* Provided user training and support, offering assistance with Linux-related queries and issues.
* Actively participated in IT team meetings and contributed to decision-making processes regarding system improvements and technology adoption.

**Education:**

Masters in computer science in University of bridgeport, CT - 2016

Bachelors in computer science aurora University - 2012

**Certification:**

Splunk Admin - 2022-02