Sheshan Gotoor

**Professional Summary**

* Over 6 years of experience in the field of IT comprising of expertise in Splunk Enterprise, and Networks and Security
* Over 2 years of experience in Splunk 6.x and Splunk 7.x as Splunk Developer.
* Extensive knowledge of Splunk Enterprise architecture and components.
* Experience setting up Indexers, Search Heads, Universal Forwarders, Deployment Server, Cluster master, and License master.
* Proficient in Splunk Search Processing Language (SPL).
* Installing and using Splunk apps for UNIX and Linux (Splunk nix).
* Experience in customizing Splunk dashboards, visualizations, configurations using customized Splunk queries.
* Configured Syslog server for the forwarding the logs to Splunk server via network protocols like TCP and UDP.
* Involved in standardizing Splunk forwarder deployment, configuration and maintenance across UNIX and Windows platforms.
* Experience in configuring routers (72xx) and switches (4500, 6500 CAT).
* Experience with Network troubleshooting and diagnosing.
* Hands-on experience with Cisco networking devices and ASA (5585-x).
* DHCP Snooping, DNS, Dynamic ARP Inspection, Zone Based Firewall.
* Technical know-how in Oracle Virtual Box, VMware, ASDM, Wireshark, Network Miner, and Cisco packet tracer.
* Strong Knowledge of TCP/IP and OSI models, and Security concepts like IDS/IPS.
* Extensive Experience in CLI, Python, R, and C.
* Proficient in shell scripting(Bash), Java and Perl.
* Familiar with Windows, Mac OS, Linux (Red hat, Ubuntu and Kali Linux) and Metasploit.
* Strong technical background in understanding and analyzing Malwares.
* Working knowledge of HTML, CSS, PHP, SQL.

**Certifications**

* **Splunk Core Certified Power User**.
* **Splunk Core Certified User**.
* **Cisco Certified Network Associate (CCNA).**

**Work Experience**

**Splunk Consultant/Admin (08/2018 – present)**

* Installed and setup the entire Splunk Components and Infrastructure.
* Helped acquire the Splunk license, and was an integral part of the discussion regarding the license size and its purchase.
* Deployed clustering techniques for indexers for high availability of event logs.
* Created real time dashboards, reports and scheduled reports.
* Worked with summary indexing to help improve search performance.
* Trained the application teams on creating dashboards, reports, and alerts.
* Setup the deployment server for forwarder management.
* Setup the Cluster master for indexer management.
* Configured multiple .conf files to better customize and improve Splunk performance.
* Standardized and implemented splunk Universal Forwarder deployment, configuration and maintenance in linux and windows platforms.
* Involved in index management, configuration files, user and role access for various applications.
* Helped Create and setup alerts to monitor the environment and data input.
* Conducted training sessions on Splunk management and SPL for the technical teams.

**Environment:** Splunk 7.2, Ubuntu, AWS, Windows, Redhat, Splunk UF, Jboss.

**Splunk Developer/Admin (08/2017-07/2018)**

**Legg Mason.**

* Installed and configured and administered Splunk Enterprise and Splunk forwarders on different environments.
* Optimized splunk performance by separating indexing and search heads across different machines.
* Maintain and manage the search head and index clusters.
* Administered and help install Universal Forwarders on diverse geospatial servers to forward log events to the indexer clusters.
* Participated in identifying, designing and building Splunk dashboards.
* Installing and using splunk apps for UNIX and linux (splunk UNIX).
* Created historical and real-time Dashboards, reports, scheduled searches.
* Helped Create and setup alerts to monitor the environment and data input.
* Created and managed Data models using CIM add-on, and helped users acclimate to the Pivot tool to create reports using Data models.
* Worked with props.conf and transforms.conf files to reduce license costs by redirecting all unnecessary log events to ‘null queue’.
* Developed user roles to complement Security and operational utilization.
* Established indexes and retention policy of buckets.

**Environment:** Splunk 6.7, AWS, Windows 2008 R2, Windows 2012 R2, Splunk UF, Redhat Linux, Navisite, Knowledge Objects.

**Splunk Developer (11/2016-07/2017)**

**Suntrust.**

* Created Splunk Search Processing Language (SPL) queries, reports, alerts and dashboards.
* Troubleshoot and resolve Splunk performance, log monitoring issues, and dashboard creation.
* Worked with knowledge objects like tags, Lookups, macros for search query optimization.
* Standardized and implemented Splunk Universal Forwarder deployment, configuration and maintenance in Linux and Windows platforms.
* Created detailed reports and scheduled reports as required.
* Created and setup alerts to monitor server activity/inactivity and to identify trends.
* Setup splunk forwarders for new application tiers introduced into the environment and existing applications.
* Used inputs.conf and outputs.conf fies for forwarder management.
* Developed and created dashboards in coherence with multiple departments and application teams.
* Assist users with creation of dashboards.
* Performed field extractions and transformations using RegEx in Splunk.
* Provide recommendations, guidance and support in the technical development of new or less experienced team members.

**Environment:** Splunk 6.2, CIM add-on, Apache 2.x, python, RegEx, Splunk Knowledge Objects

**Research Engineer (01/2016 – 11/2016)**

**Auburn University.**

* Created a toolbox for machine learning in Neuro-Imaging (MALINI).
* The toolbox was developed using Python and matlab.
* Toolbox will be made open source after the paper is published.
* Developed an algorithm in R using gradient boosting to predict mental disorders in post war veterans.
* Despite limitations in quantity of training data, the algorithm predicted with an accuracy of up to 60%.
* Worked on classification and regression based algorithms.
* Responsible for implementing data mining and statistical machine learning solutions.
* Conducted t-test and correlation between multiple neuro-imaging datasets.
* Helped publish three papers in different scientific journals.

**Environment:** Python, R, Matlab, Machine Learning, SPM, Redhat Scripting.

**Network Security Engineer (01/2013 – 01/2016)**

**Exceed Management.**

* Configuring and troubleshooting routing to establish and maintain end to end network reachability.
* Implemented a comprehensive security policy involving routers, switches and firewalls.
* Designed IP addressing schemes, VLAN’s, subnetting and trunking as per requirements.
* Configuring Routers and switches security features as required.
* Configured ACL to allow only authorized users.
* Worked with security devices to deploy VPN and IDS services.
* Monitored and responded to security incidents using splunk and wireshark.
* Used Python and Redhat linux scripting to further analyze network captures.
* Participated in incident response, penetration testing and security assessment of applications using IBM appsan.
* Managed information and logs of network devices with SNMP and Syslog.
* Employed and used both static routing and dynamic routing protocols like EIGRP, OSPF, RIPv2 and situational redistribution.
* Diagnosed and resolved networking tickets.

**Enivornment:** Cisco 7200 Router, 4500, 6500 CAT Switches, 5585 ASA, Vmware, Wireshark, TCPdump, IBM appscan, Python, Redhat, Cisco IOS.

**Education**

**Masters of Science**, Auburn university, AL.

Computer Engineering.

**Bachelors of Technology**, JNTUH

Electrical and Electronic Engineering.