Splunk Content Developer/Admin Splunk Content Developer/Admin Splunk Content Developer/Admin - Equifax Over 6+ years of experience, in field of SIEM Information Security with expertise in Implementation and Operation phases of the project. Extensive experience in deploying, configuring and administering Splunk clusters. Expertise in Actuate reporting, development, deployment, management and performance tuning of Actuate reports Created Splunk app for Enterprise Security to identify and address emerging security threats through the use of continuous monitoring, alerting and analytics. Helping application teams in on-boarding Splunk and creating dashboards, alerts, reports etc. Perform Field Extractions and Field Transformations using the Regular Expressions in Splunk. Write complex IFX, REX and MULTIKV command to extracts the fields from the log files Setup Splunk Forwarders for new application levels brought into environment. Develop custom app configurations (deployment-apps) within SPLUNK in order to parse, index multiple types of log format across all application environments. System Administration familiar with Windows Servers, Red Hat Linux Enterprise Servers. Experience in Shell scripting and extensively used Regular expressions in search string and data anonymization. Created dashboards, report, scheduled searches and alerts, SIEM searches and alerts Metrics related to AWS Created correlation searches through Splunk enterprise security. Good Understanding of configuration files, precedence and daily work exposure to Props.conf, transforms.conf, inputs.conf, outputs.conf and Setting up a forwarder information based on requirement. Experience in Optimized search queries using summary indexing. Experience in Designing and implementing Trend Micro Excellent analytical and interpersonal skills and ability to learn new concepts and supported 24/7 on call in production and development environment. Developed dashboard for manager/director level use to monitor real time security incidents and notable review in Splunk ES Work Experience Splunk Content Developer/Admin Equifax - Atlanta, GA June 2017 to Present Configuring various Dashboards/Reports and schedule PDF delivery to respective teams using Splunk. Word around updating Splunk 6.x to 7.x version. Created around 10-15 Dashboards mostly based on security related. - Developed endpoint Dashboard to track all the threats coming in and to track what servers and computers are infected. Developed

Director/Manager level dashboards to track how many incidents analysts are working and how many malware related alerts triggering on daily basis. Created correlation searches for security incidents through Splunk enterprise security Work around different log sources like Firewall, VPN, DNS, AV, Proxy Logs. Created custom dashboards for Splunk Enterprise Security where analyst can monitor threats more effectively. Created some advanced visualization Dashboards using JavaScript and XML. Designing and implementing Splunk-based best practice solutions. Developed Splunk infrastructure and related solutions as per automation toolsets. Installation and configuration of Splunk product in different environments. Configured Splunk Searching and Reporting modules, Knowledge Objects, Administration, Add-On's, Dashboards, Clustering and Forwarder Management.

Designing and maintaining production-quality Splunk dashboards. Splunk Enterprise Deployments and enabled continuous integration on as part of configuration management. Involved in Installation, Administration and Configuration of Splunk Enterprise and integration with local legacy systems. Used Splunk DB Connect Addon to integrate Splunk with Database like SQL Expertise in creating and customizing Splunk applications, searches and dashboards as desired by IT teams and business. Drive complex deployments of Splunk dashboards and reports while working side by side with technical teams to solve their integration issues. Experience in working with Splunk authentication and permissions and having significant experience in supporting large scale Splunk deployments. Splunk configuration that involves different web application and batch, create Saved search and summary search, summary indexes. Designed and Built Tomcat environment in Stage, Dev and Production environment Created and Managed Splunk DB connect Identities, Database Connections, Database Inputs, Outputs, lookups, access controls. Experience on Splunk search construction with ability to create well-structured search queries that minimize performance impact.

Parsing, Indexing, Searching concepts Hot, Warm, Cold, Frozen bucketing. Configured and setup Secure Sockets Layers (SSL) for data encryption and client authentication. Installed and configured Splunk DB Connect in Single and distributed server environments. Experience with Splunk Searching and Reporting modules, Knowledge Objects, Administration, Add-On's, Dashboards, Clustering and Forwarder Management. Well versed in both remote and on-site user

Splunk Support. Building Searches and visualize them using dashboarding capabilities of Splunk as per business requirements. Created security-based alerts in Splunk and notable events in Splunk incident review page Experienced in creating and running Cron Jobs for scheduled tasks. Involved in handling various Incident and request related to the application. Extensive experience in Python web frame works like Django, Pyramid and Flask in implementing MVC, singleton, factory architecture. Designed the Web application Using Python on Django Web Framework pattern to make it extensible and flexible Developed shell scripts to handle everyday System Administration tasks such as backup procedure, system cleanup, everyday system tasks, log rotation etc. Created notable security related events and custom dashboards in Splunk es. Configured Splunk Searching and Reporting modules, Knowledge Objects, Administration, Add-On's, Dashboards, Clustering, and Forwarder Management. Performed troubleshooting, fixed and deployed many Python bug fixes of the main applications that were sources of data for both customers and internal customer service team. Skilled in using collections in Python for manipulating and looping through different user defined objects. On a scheduled basis, configure backups, verify custom reports, manage log source groups, and validate log sources with client. Splunk Admin/Developer Orange Wings Aviation, Lauderdale, FL September 2016 to May 2017 Created Dashboards, Visualizations, Statistical reports, scheduled searches, Alerts and worked on creating different other knowledge objects. Worked on installing Universal and Heavy forwarder to bring any kind of data fields in to Splunk. Provide Regular support to Splunk project teams on complex solution and issue resolution. Helping application teams in on-boarding Splunk and creating dashboards/alerts/reports etc. Maintained and managed assigned systems, Splunk related issues and administrators. Involved in admin activities and worked on inputs.conf, index.conf, props.conf and transform.conf to set up time zone and time stamp extractions, complex event transformations and whether any event breaking. Involved in standardizing Splunk forwarder deployment, configuration and maintenance across UNIX and Windows platforms. Designing and maintaining production-quality Splunk dashboards. Create Dashboard, Reports and Alerts for events and configure alert mail. Worked on DB Connect configuration for Oracle and MySQL Developing

Scheduling Alerts, Experience with Deployment Server & Advanced XML. Created Dashboards for various types of business users in organization and worked on creating different Splunk Knowledge objects like Macros, IFX, Calculated fields, Tags, Event Types and Look ups. Field Extraction, Using IFX, Rex Command and Reg Ex in configuration files. Use techniques to optimize searches for better performance, Search time field extractions. And understanding of configuration files, precedence and working. Developed dashboards to monitor Splunk issues like skipped searches and performance issues. Various types of charts Alert Settings Knowledge of app creation, user and role access permissions. Creating and managing app, Create user, role, Permissions to knowledge objects. Splunk Developer Comcast - Philadelphia, PA March 2016 to August 2016 Expert in Extracting, Transforming, Analyzing, Visualizing, and presenting data from diverse business areas in insightful ways to enable IS Managers and Directors to take actions. Built various types of charts, reports, dashboards, alerts, managed user, role access permissions and permissions to knowledge objects. Various types of charts Alert Settings Knowledge of app creation, user and role access permissions. Creating and managing app, Create user, role, Permissions to knowledge objects. Developed robust, efficient queries that will feed custom Alert, Dashboards and Reports. Worked on Splunk search processing language, Splunk dashboards and Splunk dbconnect app. Publishing data into Splunk through configurations such as inputs.conf, severclass.conf, server.conf, apps.conf and Outputs.conf configurations Design and customize complex search queries, and promote advanced searching, forensics and analytics Developed dashboards, data models, reports and optimized their performance. Developed Splunk dashboards, data models, reports and applications, indexing, tagging and field extraction in Splunk Created Splunk knowledge objects (e.g. fields, lookups, macros, etc.) Experience in dashboards and reports performance optimization. Developed Dashboards for Business Activity Monitoring, Enterprise Architecture Built KPIs dashboards on Patient Enrollment transactions and other business activities Built Key Performance Indicators to the Enterprise Architecture team through Splunk Created Alerts on different SLAs and thresholds through Splunk. Manipulating raw data and Field extraction Built KPIs, alerts on SLAs of filesystem services project. Business Activity

Monitoring and troubleshooting Maintain current functional and technical knowledge of the SPLUNK platform IT Security Analyst Smart Technologies - IN May 2014 to December 2015 Implemented SNMP-based networking monitoring tool CACTI, Creating Graphs, Templates, adding CAMM for TRAP Configuration, Setting Threshold. Implemented BACULA as a backup server and Scheduling backup jobs. Working on Puppet (Master & agent) for Monitoring, Reporting & Troubleshooting. UNIX/Linux Administration & Security. Installing and managing virtual machines in Esxi5 (VMWARE), VMotion, SVMotion, DRS, HA, VMware Cloning, Snapshot, creating templates, and Citrix Xen Server. Comprehensive operational knowledge of all major technology areas comprising of virtual & cloud infrastructure. Windows Administration (2003, 2008), Active Directory, DNS, DHCP. Education Master's in cyber security in cyber security Sacred Heart University - Hyderabad, Telangana Skills Database (2 years), Javascript (1 year), Python (1 year), Unix (2 years), Xml. (2 years)

Name: James Willis

Email: eweaver@example.net

Phone: +1-751-260-1333