**SRI RAM**

**646-829-9328**

**Rec2@t3incorp.com**

## **PROFESSIONAL SUMMARY:**

6+ years of experience in Splunk configuring, implementing and supporting Splunk Server Infrastructure across Windows, UNIX and Linux and in-depth knowledge of log analysis generated by various systems including security products.

* Worked on Security solutions (SIEM) that enable organizations to detect, respond and prevent these threats by providing valuable context and visual insights to help you make faster and smarter security decisions.
* Experienced in SIEM (Security Information and Event Management) of Splunk and sound knowledge on other offering Technologies in the market like QRadar.
* In depth and extensive knowledge of Splunk architecture and various components (indexer, forwarder, search head, deployment server), Heavy and Universal forwarder, License model.
* Monitoring Splunk Infrastructure (Identify bad searches, dashboards and overall health of Splunk) and collaborate with respective teams to improve performance.
* Developed and implemented business rules for automated and manual process using access policies and approval workflows according to business needs.
* Experienced in optimizing the Splunk Forwarder management architecture through a centralized server to manage the configurations
* Experienced in Perl and Pythonscripting languages
* Used various Splunk Apps such as Splunk on Splunk, Universal Field Extractor, Splunk App for   
  UNIX/Linux, Splunk DBI Connect.
* Developed customized application configurations in Splunk to parse, index multiple types of log format across all application environments.
* Developed customized Shell scripts to install, manage, configure multiple instances of SPLUNK   
  forwarders, indexers, search heads, deployment servers.
* Self-motivated, innovative, Dedication, willingness to travel & relocate and ability to adopt and learn new concepts and technologies.
* Good knowledge on protocols like HTTP,FTP SSH, SMB.
* Experience in Security Incident handling SIEM using RSA Envision and IBM Qradar products Identifying the critical IT infrastructure that requires 24/7 monitoring.

## **TECHNICAL SKILLS:**

|  |  |
| --- | --- |
| Monitoring Tools | SPLUNK 6.0, SPLUNK 6.2, SPLUNK 6.3.3,SPLUNK 6.4, QRadar |
| Operating System | Ubuntu Linux, Red Hat Linux, Oracle Enterprise Linux, Solaris and Windows 98, 2000, XP, 7, 8 , and 10. |
| Web technologies | HTML, CSS, JavaScript, XML, Advanced XML |
| Programming | SQL, PL/SQL, SQL Plus, Unix Shell Scripting, C, Java. |
| RDBMS/Database Servers | Oracle 11g/10g/9i/8i, MS SQL Server 2012/2008/2005/2000, MS Access. |

## **PROFESSIONAL EXPERIENCE:**

**American Express, Phoenix, AZ**Feb 2017 - Present

**Role: Splunk Admin/Developer**

**Responsibilities:**

* Involved in standardizing Splunk forwarder **deployment**, **configuration** and maintenance across **UNIX** and **Windows** platforms.
* **Monitored** Splunk Infrastructure for capacity **planning** and **optimization**.
* Use Splunk Enterprise Security to configure correlation search, key indicators and risk scoring framework.
* Supported 6+ Splunk search Heads, 30 + Indexers, 2500 + forwarders
* Good understanding of **security threats** and **vulnerabilities** and how to detect and mitigate them, experience in building security monitoring and incident management solutions using Splunk.
* Created various types of charts **Alert settings** Knowledge of app creation, user and role access permissions.
* Experienced in working with **Splunk authentication** and permissions and having significant experience in supporting large scale Splunk deployments.
* 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.
* Knowledge about Splunk architecture and various components (indexer, forwarder, search head, deployment server), Heavy and Universal forwarder, License mode
* Created Dashboards, Visualizations, Statistical reports, scheduled searches, alerts and also worked on creating different other knowledge objects.
* Experienced on Security Information Event Management and good knowledge on information security products (Firewalls, IDS/IPS)
* **Designing** and **maintaining** production-quality Splunk**dashboards.**
* Extensively used App Dynamics to monitor CPU, memory usage, JVM heap memory health, session and thread counts, and application log error.
* Understanding client business requirement and translating into technical requirement and use cases.
* Documented standards, best practices and Operating procedures.
* Very good understanding of software development life-cycle (SDLC) process, Followed Agile scrum and story maps for dev tracking.
* Integrate Service Now with Splunk to consume the alerts from Splunk and create service now tickets.

**Environment**: Splunk 6.x, Splunk ES, Splunk DBConnect2.0, Splunk ITSI, Splunk ITOA, D3.js, Tomcat 7.x, JBoss 7.x, BIGIP Load Balancers, SAML, Configured plug-ins for Apache HTTP server 2.4, RedHat Linux 6.x, JDBC, JDK1.7, J2EE, JSP, Servlets, XML, Oracle 11g, GI.

**Bank of America, Chicago, IL**June 2016 –Jan 2017

**Role: Splunk Admin/Developer**

**Responsibilities:**

As primary for Splunk support, supported Splunk circulated environment comprising of search heads, indexers and forwarders across different OS including Aix, Solaris and Windows.   
• On boarding the data from different application servers kept across the globe to the Splunk Server.   
• Created Splunk app for Enterprise Security to identify and address emerging security threats through the use of continuous monitoring, alerting and analytics.   
• Troubleshooting and resolve the Splunk - performance, log monitoring issues; role mapping, dashboard creation etc.   
• Configured Indexer replication to achieve data availability, data fidelity and disaster tolerance.   
• Improved search performance by configuring search heads for all Indexes in production.   
• Install different Splunk Applications, for example, Cisco for Splunk, Windows for Splunk and VMware for Splunk.   
• Created Shell Scripts to install Splunk Forwarders on all servers and configure with common configuration files such as Bootstrap scripts, Outputs.conf and Inputs.conf files   
• Configured Splunk forwarder to send unnecessary log events to "Null Queue" using props and transforms configurations to reduce license costs.   
• Created and configured management reports and dashboards in Splunk for application log monitoring.   
• Provided load/stress and architecture validation testing and troubleshooting on issues such as Out of Memory, 100% CPU Usage hung Thread sessions, session replication, JVM Crashes.   
• Efficiently handled Work Load Management for load balancing and failover, improving performance, reliability and scalability.   
• Gathering different wellsprings of syslog and XML information from different gadgets, applications, and information bases.   
• Setup Splunk Forwarders for new application tiers introduced into environment and existing applications.   
• Work closely with Application Teams to create new Splunk dashboards for Operation teams using advance XML and CSS.   
• Supporter and execute arrangements considering a full information lifecycle (Search & Investigate, Add Knowledge, Monitor & Alert, Report & Analyze).   
• Expertise in Fetching the data from databases using "DB Connect Application"   
• Efficiently fixed Event breakings and Time zone issues.   
• Worked on Network Firewalls, Load-balancers, LDAP and complex network design.    
**Environment:** Splunk 5.1.2, XML, Linux, Bash, Splunk ITSI, Splunk Forwarder 5.x/6.x, Perl, Oracle 11g, CSS, JavaScript, WebLogic Server 11g/10.x, VMware, Windows, operations analysis, Regular Expressions.

**Info solutions, HYD, India** March 2013 - Feb 2015

**Role: Splunk Engineer**

**Responsibilities:**

• Must have strong Splunk UI experience and able to debug expensive search queries.   
• Understands Splunk configuration and able to debug Splunk related issues.   
• Setup splunk Forwarders for new application environments and also for existing applications.   
• Involved in standardizing Splunk forwarder deployment, configuration and maintenance across UNIX and Windows platforms.   
• Good experience with scripting languages like perl, python and bash.   
• Design solutions and concepts for data aggregation and visualization.   
• Work with a small team to enhance the existing Infrastructure.   
• Solve complex Splunk Integration challenges.   
• Debug complex Splunk configuration issues.   
• Maintain or bring in industry standards in network and storage solutions.   
• Build Splunk apps from ground up for Splunk to interact with 3rd party software/hardware.   
• Communicate with peers and supervisors routinely, document work, meetings, and decisions   
• Work within a Project Team environment   
• Understand and promote the quality policy.   
• Define process for centralized application log file ingestion into Splunk   
• Identify the amount of work needed to ingest, interrogate and map log files correctly   
• Identify critical data elements that must be present to ensure log files can be used for monitoring & Define desired format for log files to be used   
• Define a mapping & exception process for those log files that cannot be generated in the desired format   
• Perform log interrogation to determine elements   
• Perform mapping/parsing in Splunk for various log feeds   
• Inventory current log feeds in Splunk   
• Define process to keep inventory updated as new feeds come in   
• Experience in working with Splunk authentication and permissions and having significant experience in supporting large scale Splunk deployments   
• Interacted with the data warehousing team regarding extracting the data and suggest the standard data format such that Splunk will identify most of the field

**Environment**: SPLUNK , Linux, UNIX, MS SQL Server, Splunk Enterprise Security

## **Education:**

Master of Science in Computer Information Systems (MSCIS) from Californian university of management and Sciences – 2016 3.72 GPA.

Bachelor in Sciences from MGR University 2011.