**Tunde Akinsola**

Houston, TX 77063

(857) 333 6942

akinsolabat@gmail.com

**Professional Summary:**

* Self-motivated, responsible, knowledgeable, detailed oriented IT security monitoring engineer with proven success in IT System Management, RHEL Linux, Solaris, Windows Servers, and Databases.

**Technical Skills:**

* GIT, GitHub, Jenkins, Jira, Heat, Linux (Red hat), Unix, Windows Servers, Databases, Apache, Apache web server, apt, Backup, BIND, CLI, clustering, Network systems, config, Databases, Database, debugging, Routers, Switches, DHCP, Disaster Recovery, DNS, Firewall, SFTP, GUI, SMTP, LAN, LDAP, Linux, logging, Access, mail, Windows, Migration, modeling, MySQL, NFS, Servers, scripts.

**Professional Experience:**

**Department of Veterans Affairs (TISTA). Houston, TX**

**November 2021 – July 2022**

**Senior Software Engineer (Splunk)**

* Design Splunk Deployments.
* Perform Network configuration of new appliances.
* Perform Splunk admin jobs including installing, configuring, tracking, and tuning.
* Configuration of extension modules like the Switch Module and Splunk Module.
* Test network security product such as firewall, intrusion prevention systems, and SIEM solution.
* Support development and maintenance of the data center information security program.
* Monitor, evaluate, and maintain systems and procedures to protect data systems and databases from unauthorized access.
* Create Dashboards, Visualizations, Statistical reports, scheduled searches, signals, and knowledge objects.
* Integrate event feeds from client specific event sources into Splunk.
* Provide suggestions and implement modifications to optimize Splunk product in client environments.
* Write and expand custom scripts, applications as needed.
* Engage with customers to collect requirements, carry out troubleshooting, and offer help with the creation of Splunk search queries and dashboards.
* Manage Splunk environments for customers with emphasis on infrastructure, overall performance monitoring, and security solution
* Onboard data into client Splunk environments – both Splunk Cloud and Enterprise
* Work customer tickets from clients inside agreed upon service level agreements (SLAs)
* Build new customer environments as required
* Create monitoring and alerts that proactively screen client environments use cases, correlation rule sets, and content definitions primarily based totally on several intelligence and detection products.

**Department of Veterans Affairs, (Leidos). Houston, TX**

**August 2020 –** **November 2021**

**Senior Software Engineer (Splunk)**

* Developed use cases, correlation rule sets, and content definitions based on numerous intelligence and detection products.
* Designed, developed, and reviewed complex SIEM content based on endpoint events, network events, and threat intelligence feeds (IOCs).
* Perform Splunk admin jobs including installing, configuring, tracking, and tuning.
* Configuration of extension modules like the Switch Module and Splunk Module.
* Test network security product such as firewall, intrusion prevention systems, and SIEM solution.
* Worked with security analysts, intelligence analysts, security operation engineers, and various teams to continuously improve published content.
* Participated in new events development/testing, developed methodology of investigation and documentation before the new event introduced into SOC queue while closely interacting with Incident Response teams.
* Security use cases design, implementation, and management: threat modeling, continuous content delivery (detections) and management (JIRA).
* Designed and implemented highly customized correlation rules, reports, regular expression parsers, trends, and dashboards.
* Responsible for Information Security Threat Management Program which includes Threat Intelligence, Threat Modeling, Threat Hunting, and Security Analytics.
* Participated in the SIEM Review Board and SIEM tuning meetings; made recommendations for tuning as applicable
* Analyzed threat information from multiple sources, disciplines, and agencies across the regulatory and Intelligence Communities. Synthesizes and places regulatory and intelligence information in context; draws insights about the possible implications.

**SYSCO Corporation, Houston, TX**

**May 2017 – June 2020**

**Splunk Engineer**

* Utilized knowledge objects for reporting statistics.
* Utilized the Distributed management console to investigate resource usage.
* Script deployment of universal forwarder Agent to 300 application servers.
* Configured license pooling.
* Maintained high available of index data by clustering the indexer.
* Maintained replicating copies of all knowledge objects by clustering search head.
* Troubleshot Splunk feed issues and data ingestion for remote locations.
* Deployed new Splunk architecture at disaster recovery site.
* Configured hot, warm, and cold buckets hold data for extended period of time.
* Created home dashboards to monitor ingestion and feeds for private network performance.
* Gave presentation to other System admins on how to effectively use Splunk for troubleshooting.
* Designed and implemented syslog network traffic and syslog server.
* Installed and configured deployment server and search head deployer.

**United States Army, Fort Carson, CO**

**Apr 2015 – Apr 2017**

**Security Technician**

* Engineered systems administration-related solutions for various project needs
* Installed and configure systems which support infrastructure and/or activities.
* Developed and maintain installation and configuration procedures.
* Contributed to and maintain system standards.
* Contributed to and maintain security posture of the system
* Researched and recommended innovative, and where possible, automated approaches for system administration tasks. Identified approaches that leverage resources, Operations and Support.
* Installed and maintained security patches on the operational and development system.
* Reported Security Patch compliance.

**Direct Energy, Houston, TX**

**Sept 2012 – Mar 2015**

**System Admin**

* Experienced in System Administration, Installation, Upgrading, Patches, Migration, Configuration, Troubleshooting.
* Troubleshot connectivity to Servers and Network systems.
* Installed and configured Splunk in a staging environment.
* Managed Security, Backup, Disaster Recovery, Performance Monitoring and Fine-tuning on Linux (RHEL) systems.
* Experienced using Red Hat Satellite server to deploy, monitor, update, and manage systems.
* Automated Patching using Errata and customized security patching using Ksplice.
* Involved in complete Administration tasks on Red Hat Linux and documentation for the projects executed.
* Installed, monitored, and supported Web and Application Servers on Linux environments.
* Good knowledge on operating systems architectures.

**Certification:**

* PMP
* CISM
* CISA
* Security +
* AWS Certified Security – Specialty
* Splunk Core Certified User
* Splunk Core Certified Power User
* Splunk Enterprise Certified Admin
* Splunk Enterprise Security Admin

**Education:**

* MSc Project Management – 2015
* MSc Geographic Information Systems - 2010
* B.Sc. (Hons) Geology - 2007