Oluwaseun Ojimi

Virginia | 540-429-6676 | oluwaseun.ojimi1@gmail.com

SIEM/SPLUNK/DATA ENGINEER

Professional Summary

Dedicated and results-driven IT professional with extensive experience in Azure environments, specializing in KQL and possessing a wealth of knowledge in Splunk. Proven track record of designing, implementing, and optimizing Splunk, Azure solutions to meet business objectives. Seeking a challenging role where I can leverage my expertise to drive innovation and contribute to the success of a dynamic organization

Education

Western Governors University **Salt Lake City, UT**
Master of Science, Data Analytics **[May 2022]**

Morgan State University **Baltimore, MD**
Bachelor of Science in Civil Engineering **[May 2017]**

Technical Skills:

- Azure: Azure Monitor, Azure Arc, Logic apps, Microsoft Sentinel
- Splunk: Enterprise, Cloud, Security
- Operating Systems: Linux, Windows, macOS
- Scripting Languages: Bash, Python, PowerShell, YAML
- Databases: Oracle, SQL Server, MySQL
- Tools: Jenkins, Git, Ansible, Docker, Kubernetes, AWS, Jira, remedy
- Security: SIEM, IDS/IPS, Firewall, SOC
- proficient in Azure services and solutions (Log Analytics, Azure Monitor, Azure Logic Apps, Microsoft Sentinel, Deployment Scripts)
- Strong Knowledge of KQL (Kusto Query Language) and SPL (Search Processing Language)
- Experienced in Splunk Enterprise and Splunk Enterprise Security
- Excellent Problem-solving and troubleshooting skills.
- Strong communication and collaborations skills.

Splunk Certifications

- Splunk Enterprise Certified Architect
- Splunk Enterprise Certified Admin
- Splunk Core Certified Power User
- Splunk Core Certified User

Work Experience

Powerhouse Institute Inc | Census Bureau **Bowie, MD**

Splunk Engineer / Azure Cloud Analyst February 2022 – Present

Azure

- Manage, and deploy azure based solutions, including virtual machines, Azure log analytics, Azure logic apps, Microsoft Sentinel and Azure Arc.

- Develop and optimize KQL queries to extract actionable insights from Azure monitor, Log Analytics, and Application insights.
- Automate routine tasks and workflows using Azure Logic apps, Azure Automation and Azure functions.
- Develop security KQL queries and threat detection to enhance the security posture of Azure environments.
- Collaborate with cross-functional teams to troubleshoot and resolve Azure- related issues and optimize performance.
- Conduct data onboarding tasks and create workflows into Azure Log Analytics using Azure Automation and Azure functions, streamlining the process of ingesting logs from various sources.
- Conduct regular audits and assessments of data onboarding processes to ensure compliance with industry standards and best practices, optimizing the efficiency and effectiveness of log management in Azure environments.

Splunk

- Installed, configured, and maintained Splunk Enterprise and Splunk Universal Forwarders across distributed environments.
- Developed and optimized complex Splunk queries and dashboards to monitor system performance, security events, and application logs.
- Implemented Splunk Enterprise Security for advanced threat detection, incident response, and compliance reporting.
- Managed Splunk user access and permissions, ensuring adherence to security policies and regulatory requirements.
- Provided technical expertise and support to internal teams for troubleshooting and resolving Splunk-related issues.
- Conducted Splunk training sessions for IT staff to enhance their proficiency in using Splunk for log analysis and monitoring.
- Created custom dashboards and reports to visualize security metrics, trends, and key performance indicators for executive reporting and decision-making
- Participated in incident response activities, leveraging Splunk ES capabilities to analyze and mitigate security breaches and incidents promptly.
- Conducted regular tuning and refinement of security content to enhance detection accuracy and reduce false positives.
- Developed and maintained correlation searches, notable events, and alerts within Splunk ES to detect and respond to security incidents in real-time.

Work Experience

Feddata LLC | IRS **Kearneysville, WV**

Splunk Engineer / Admin /Developer August 2020 – January 2022

- On boarded new applications data into multi-site Splunk environment
- Developed Splunk searches and knowledge objects targeted at understanding application performance and security analysis.
- Experience with providing regular support guidance to SOC project teams on complex solution and issue resolution with the objective of ensuring best fit and high quality.
- Contents creation/dashboard development using dashboard studio
- Created security indictors monitoring dashboard that compares threats indicators listed in the STIX/TAXII/Lookingglass Cyber feed against all Ip traffic seen in the environment.
- Participate in on-call rotation to provide 24/7 support for critical incidents.
- Maintain documentation and knowledge base for Splunk environments.
- Involving and assisting other teams with issue identification and resolution utilizing splunk/monitoring platforms
- Build Splunk custom apps, add on, use REST API for props inputs, scripted inputs and incorporate custom commands
- Engaged with Splunk support/PS for various Splunk issues and Splunk licenses.
- Expertise in Preparing, arranging, and testing the Splunk search strings and operational strings.
- Experience in developing Splunk queries and dashboards targeted at understanding application Performance and capacity analysis.

Jacobs Technology Inc | Federal Student Aid (FSA) **Washington, DC**

Splunk Engineer August 2019 – August 2020

- Splunk contents infrastructure development
- Developed ansible playbook that fixes the issue of date time data ingested on or after Jan 1, 2020.
- Provide regular support guidance to SOC project teams on complex solution and issue resolution with the objective of ensuring best fit and high quality.
- Investigated failed jobs and writing SPL to debug data load issues in production
- Monitored license usage, indexing metrics, index performance, forwarder performance.
- Communicate with peers and supervisors routinely, meetings, document work
- Performing support on splunk and monitoring platform components.
- Expert in extraction of fields (SIEM Compliance)
- Expert in installing SPLUNK apps for Linux and UNIX environments.
- Configured files in Splunk (props.conf, Transforms.conf, Output.conf)
- Onboarding of network devices data from different security tools into Splunk Infrastructure.
- Creation of separate indexes for different devices as per Client policies
- Creation of local users on Splunk with appropriate access rights.

Jacobs Technology Inc | Department of Health and Human Services **Washington, DC**

Splunk Engineer February 2019 – August 2019

- Performed investigation into causes of Performance degradation.
- Consult with Dashboards/report developers and end users to address problem areas and reduce search head saturation
- Collaborate with Business team to establish best practice documentation and governance for searching, reporting dashboarding for distribution to all consultant business and IT users.
- Leverage performance analysis to provide guidance on tuning consultant platform configuration
- Deployed bloodhound app for analysing users searches behaviour and scheduler activities
- Provide implementation guidance and support
- Creating and publishing weekly/monthly reports using excel, word and Splunk.
- Created the reports and saved searches for the improvement of Splunk performance by using complex REST API and regex.
- Used python script to ingest jira data into splunk infrastructure
- Dealing with Splunk Utilities like bucket rolling, user index creation and management, Source type, forwarder log monitoring input, output, and props configuration.
- Used Splunk for application log, security log and performance monitoring.
- Created python scripted inputs to generate a daily cron job that loads into Splunk for monitoring.

CLIENT: C-HIT INC. **Columbia, MD**

Splunk Admin / Engineer September 2018 – January 2019

- Involved in troubleshooting of clustering and optimizing performance
- Performed data masking of PII logs during index field extraction
- Investigated failed jobs and writing SPL to debug scheduled Jobs issues in production
- Deployed and configured Alert for Splunk Admin app for splunk environment optimization
- Contributes to the improvement of the exiting splunk processes and identification of new processes and technical alternatives to resolve problems
- Contributes to splunk infrastructure upgrade.

CLIENT: (GEICO) **Chevy Chase, MD**

Splunk Admin March 2018 – September 2018

- Deploying splunk apps and configuration form the deployment server
- Developing environment specific splunk apps based on the inputs from application enterprise business team inputs.
- Time chart attributes such as span, bins, Tag, Event types, creating dashboards, reports using XML.
- Created dashboard from search, Scheduled searches of Inline search vs. scheduled search in a dashboard
- Creation of Key Performance Indicators (KPIS) in a service
- Glass Table content development
- Configuration of services as per Client policies and request.
- Scheduling saved searches and run them during a specific window of time
- Extracting fields from the data (search time) and utilizing them to create charts.
- Received appreciation from internal splunk help team and client also.
- Responsible for onboarding of network devices into Splunk Infrastructure
- Responsible for Splunk Implementation on Cloud Aws
- Onboarding of cloud trial logs from Aws cloud to Splunk Infrastructure
- Worked in a Splunk Cloud large production environment
- Experience in setting up monitoring console for all Splunk components.

Sciences Application International Corporation (SAIC) **Mclean, VA**

Splunk System Admin June 2016– January 2018

- Splunk Implementation, planning, customization, integration with Application servers, big data, statistical and analytical modelling.
- Experience in Operational Intelligence using Splunk.
- Expert in Extracting, Transforming, Analysing, Visualizing, and presenting data from diverse
- Great understanding in using regex to extract key value
- Configured monitoring console for proper management of our splunk environment
- Created best practices retention policy with our environment
- Design and configure splunk indexers clustering for high availability
- Implemented Splunk architecture and its various components (indexer, forwarder, search Heads, deployment server), Heavy and Universal forwarder, License model.
- Various types of charts Alert settings Knowledge of app creation, user and role access permissions.
- Connecting and indexing data from relational database such as Oracle DB2
- Creating and managing app, Create user, role, Permissions to knowledge objects
- Created standard operating procedure SOPs
- Create data retention policies and perform index administration, maintenance, and optimization
- Ability to troubleshoot splunk infrastructure components in highly available, multi-site design

PROJECT DESCRIPTION

- ❖ Implementing performance monitoring and analytical tool in enterprise environment to test application and webserver performance and testing the application behaviour in splunk enterprise environment.
- ❖ Support the environment whenever they are facing issues in the prod or non-prod environment analysis the issue and narrow down the cause and resolve it as soon as possible.
- ❖ Monitor application instances and their performance using this tool and performance tuning the environment and improve the business.

Verizon **Silver Spring, MD**

Linux Junior System Admin June 2015– May2016

- VMware Administration and Operation including Virtual Desktop
- Monitoring application process
- Establishing new security processes
- Performed User Accounts Administration
- Storage (RAID Configuration)
- Enterprise monitoring REMEDY
- Installed Sun recommended patch cluster
- Execute scripting in a production environment.
- Installing and configuring the Splunk software on Linux virtual machines
- Creating and modifying splunk App
- Viewing process logs with Splunk
- Splunk Dashboard Development and Infrastructure Monitoring
- Implement monitoring within Splunk
- Creating user account and permission on splunk enterprise
- Setting up and ingestion of various data flows to include pre-processing data into a useable/readable format
- Migration of non-clustered indexers to a clustered environment
- Ability to customize Dashboards via the XML source

Pricewaterscoopers **Baltimore, MD**

Software Engineer Associate June 2013– May 2014

- Dealt with VALANG data type related issues and functional part of LMOP application (Helpdesk).
- Developed Junit tests to introduce software validation message inside the LMOP application and guarantee maximum code security.
- Worked in conjunction with GHG development team to construct a dynamic web application for federal government client
- Experienced in object-oriented programming, developing, testing and debugging code.
- Dealt with designing interfaces and administering systems and networks.
- Created new fetch data quality, screen error, data completeness validation messages in different subparts.
- Converted IVP RNG checks to validation to meet customer requirement in Eggrt Application.