**Ayodeji Owoyemi**

Houston TX ,77002 | (443) 657-0638 | ayomidejiowoyemi@gmail.com

## CYBER SECURITY ENGINEER | SPLUNK ENGINEER

Experienced and certified Cybersecurity Engineer specializing in Splunk engineering with a strong track record of diagnosing and resolving technical challenges in multi-user environments. Proficient in various Splunk versions, monitoring tools like Dynatrace, AppDynamics, and NAGIOS/Nimsoft, and skilled in Python, I develop and design customized dashboard control panels for customers and administrators using Django, OracleDB, PostgreSQL, and VMWare API calls. Seeking to leverage my expertise and passion for cybersecurity to fortify organizations against modern cyber threats, conduct risk assessments, and contribute to proactive cybersecurity measures. Master's degree and relevant certifications in hand.

Dynamic and results-oriented marketing professional with extensive experience in customer engagement, product demonstration, and technical content creation. Proven track record of leveraging data analytics tools, like Splunk, to drive marketing strategies and improve customer experience. Adept at translating complex technical concepts into clear, persuasive marketing materials. Excellent presentation and communication skills

## TECHNICAL SKILLS

**Operating Systems:** Red Hat, Windows 2000 Professional, Windows XP, Windows NT 2003 Server, HPUX

**Virtualization:** VMware vSphere Vcenter, VMware ESXi 4x, 5x

**Monitoring Tools:** OSSEC, NAGIOS/Nimsoft, Dynatrace, AppDynamics, Chronicle

**Databases:** OracleDB, PostgreSQL, MySQL, MS SQL

**Scripting:** Python, Bash shell scripting

**Security:** Splunk Enterprise, Hadoop, APM/Monitoring tools, Nessus, Wireshark, Cisco ASA, Sourcefire

**Other Tools:** Ansible, Chef, Puppet, Websense, Tripwire, Marketing Strategy, Customer Engagement, Product Demonstration, Technical Content Creation

## PROFESSIONAL EXPERIENCE

**Solution Delivery Manager**

February 2018 - Present

**Deloitte – Remote in Houston, TX**

- Designed and implemented scalable Splunk architectures tailored to meet organizational data analytics and security needs, ensuring optimal performance and reliability.
- Led the integration of Splunk with various data sources (e.g., logs, metrics, network data) to consolidate and analyze information for comprehensive insights, enhancing operational intelligence.
- Developed advanced Splunk searches, reports, dashboards, and alerts to monitor system performance, detect security incidents, and provide actionable intelligence to stakeholders.

- Engineered and maintained Splunk data models and knowledge objects (e.g., event types, tags, aliases) to improve data normalization and enrichment for accurate analysis and reporting.
- Implemented and optimized Splunk Enterprise Security (ES) for real-time security monitoring and incident response, increasing threat detection capabilities and reducing response times.
- Utilized Splunk's machine learning toolkit and predictive analytics to identify trends, forecast potential issues, and automate anomaly detection, significantly improving predictive security measures.
- Conducted Splunk capacity planning and performance tuning, ensuring the infrastructure's scalability and efficiency to handle increasing data volumes and complex queries.
- Spearheaded the development of custom Splunk applications and technology add-ons to address unique organizational requirements, enhancing functionality and user experience.
- Established best practices for Splunk deployment, configuration, and maintenance, including data retention policies and security measures to safeguard sensitive information.
- Collaborated with cross-functional teams to integrate cybersecurity frameworks and compliance standards into Splunk operations, aligning with industry regulations and best practices.
- Facilitated the transition to Splunk Cloud, overseeing migration projects to enhance system availability and accessibility while reducing operational costs.
- Delivered Splunk training and workshops to technical teams, elevating the organization's overall proficiency in utilizing Splunk for operational intelligence and security analytics.
- Acted as a subject matter expert in Splunk, providing guidance and support for complex troubleshooting, system enhancements, and strategic decision-making.
- Continuously evaluated emerging technologies and Splunk updates, integrating innovative solutions to keep the organization ahead in data analytics and cybersecurity landscapes.

**Senior principle software engineer - Splunk Dashboards –**

April 2015 – January 2018

**Dell – Houston, TX**

- Cloud managed services - building Splunk dashboards responsible for designing, implementing, and maintaining Splunk-based solutions that enable effective log management
- Maintains established platform standards for the Splunk service offering.
- Standardize Splunk forwarder deployment, configuration and maintenance across a variety of platforms.
- Apply hot fixes/upgrades.
- Led the design, development, and optimization of Splunk Dashboards, playing a pivotal role in enhancing data visualization and providing actionable insights for cybersecurity analysts and stakeholders.
- Collaborated closely with cross-functional teams, including cybersecurity experts, data analysts, and product managers, to understand user requirements and translate them into intuitive and user-friendly dashboard designs.
- Leveraged expertise in Splunk, Python, and other relevant technologies to create custom visualizations, interactive charts, and graphs that effectively conveyed complex cybersecurity data in a comprehensible manner.
- Proactively identified opportunities to improve dashboard performance, scalability, and responsiveness, optimizing data queries and implementing efficient data retrieval strategies.

- Acted as a subject matter expert on Splunk Dashboard development, providing guidance and mentorship to junior team members, and fostering a culture of continuous learning and innovation.
- Collaborated with the security operations team to identify key performance indicators (KPIs) and metrics for monitoring and measuring the effectiveness of cybersecurity controls and incident response activities.
- Designed and implemented real-time monitoring dashboards, enabling timely detection and response to cybersecurity threats and vulnerabilities.
- Conducted regular code reviews and implemented best practices to ensure the delivery of high-quality, maintainable, and secure dashboard solutions.
- Stayed abreast of the latest trends and advancements in data visualization and dashboard development, continually exploring new tools and technologies to enhance the capabilities of Splunk Dashboards.
- Acted as a key liaison between the software engineering team and cybersecurity stakeholders, facilitating effective communication and collaboration throughout the development lifecycle.
- Conducted thorough testing and validation of dashboards to ensure accuracy and reliability of displayed information, and promptly addressed any defects or issues identified during testing phases.
- Collaborated with customers and product managers to gather feedback on existing dashboard functionalities and proposed improvements, iteratively enhancing the user experience based on feedback received.
- Contributed to the documentation and knowledge sharing efforts, creating detailed technical documentation, user guides, and best practices for Splunk Dashboard development and maintenance.
- Assisted in evaluating and integrating third-party plugins and extensions for Splunk Dashboards, extending their capabilities and improving the overall functionality.

**Splunk Engineer**
June 2013 – February 2015
**Humana – Louisville, KY**

- Upgraded Splunk from version 6.5 to 7.2, performed troubleshooting on Linux servers, and set up Splunk configurations and validations.
- Developed customized dashboards, reports, and alerts to meet specific requirements.
- Onboarded network devices data from various security tools into the Splunk infrastructure.
- Installed and configured heavy, universal, and intermediate forwarders, collaborating with the Puppet team.
- Led the team in implementing intelligent Splunk solutions.
- Successfully integrated Splunk with Dynatrace using Splunk app TA and created various knowledge objects.
- Implemented separate indexes for different devices in compliance with client policies.
- Deployed Splunk apps and configurations using deployment server.
- Configured summary indexes to collect aggregated data for dashboard creation.

**Splunk Engineer**
July 2010 – May 2013
**U.S Patent and Trademark Office – Alexandria, VA**

- Installed and configured Splunk Enterprise environment on Linux, including clustered search heads and indexers.
- Created complex dashboards, forms, and visualizations using simple XML and tokens.
- Monitored security posture and incidents, analyzing both outside and inside threat vectors.
- Provided support for the Information Security Operations Center (ISOC) and analyzed various security logs.
- Managed and deployed Solaris 10, RHEL 6, CentOS 6.8, CentOS 7 servers to the network.
- Wrote bash shell scripts for process automation and performed hardening, patching, and upgrades on servers.
- Configured Apache and MySQL on Solaris 10 for web hosting and built websites.
- Troubleshot Solaris 10 hardware, software, and configuration issues.

**System Engineer**
October 2008 - March 2010
**Enterprise Linked – Beltsville, MD**

- Installed and configured services like DNS, DHCP, NFS, Apache Web Server, Samba, and SSH.
- Managed and resolved incident tickets, wrote scripts for cronjob entries, and provided assistance and documentation to the operations department.
- Assisted in troubleshooting dial-up configuration, web hosting, and domain registration issues.
- Upgraded workstations from Windows 7 to Windows 8 and resolved software and hardware issues remotely.
- Demonstrated a thorough understanding of system hardening, patching and upgrades production servers, ensuring system stability and optimal performance.

## EDUCATION & CREDENTIALS

**Master of Science in Cyber Security,** University of Maryland Global Campus
**Splunk Certified Architect 7.2**
**Splunk Certified Power User 6.5**
**Splunk Certified Admin 6.5**
**Security+**
**ITIL V3**