Debo Ajibade

Upper Marlboro, MD 20772
deboajibade5_rdi@indeedemail.com
(240) 509-0089

Security Engineer proficient in automating, optimizing, designing, architecting, configuring, and tuning Systems in cloud, virtual, and physical environments. Led Splunk integration, onboarding, migration, and upgrade efforts. Provided engineering and consultative support to Security operations.

Work Experience

Information Security Engineer (Splunk)

TechForward| ASH Group - Remote
December 2021 to Present

• Migrated Splunk from On-prem to AWS Cloud
• Subscribed, Configured & implemented AWS snowball to copy frozen data.
• Stood up, configured, and managed Multi-Site Clustered Environment
• Troubleshoot and resolve FortiGate logs volume discrepancies.
• Troubleshot syslog-ng data routing issues.
• Coordinated and implemented onboarding efforts with Security SMEs
• Built Ansible Playbook to orchestrate upgrade of Splunk.
• SAML Configuration via Azure AD
• Responsible for routing data to Multiple endpoints using a data stream.
• Implemented SC4S to ingest and parse data from Security Appliances
• Cribl: Configured leader and worker nodes for data ingestion
• Cribl: Perform data enrichment and parsing before sending data to the destination.

Senior Splunk Engineer

Gray Tier Technologies - Washington, DC
October 2018 to December 2021

• Oversaw the health of the environment and data onboarding.
• Implemented CIM via field extractions, field aliases, and eval.
• Troubleshoot Data inconsistencies from firewall devices and DNS data.
• Built a Dashboard for Post Patching testing.
• Collaborated with Security analyst to implement security content.
• Created and deployed Splunk agents with Ansible
• Index time extractions via transforms and props
• Search time extractions via regex to pull CIM-compliant fields.
• Tuned Linux Transparent Huge Pages to improve application performance.

Cyber Security Engineer/Splunk Professional Services

Defense Point Security |Remote
July 2017 to October 2018

● Implemented Clustered Splunk environment and configured instances.
● Configured search head cluster.

● Manage host files via Ansible.
● Deployed virtual machines via Vagrant for proof of concept.
● Installed User Behavior Analytics (UBA) and deployed Use Cases
● Configuration of deployer node, deployment server & cluster master
● Reviewed indexing capacity and provided capacity planning strategy.
● Configuration of Splunk LDAP authentication on search head instances

Linux Engineer/Splunk Admin

Squires Group – National Aeronautics and Space Administration (NASA) - Greenbelt, MD
April 2016 to July 2017

● Provided Linux Administration support for the ATLAS project.
● Managed High Availability Virtualized ESXI environment.
● Administered access for engineers to a Virtualized desktop environment.
● Capacity planning: accessed system resources (disk space, CPU, network bandwidth)
● Implemented backup & patch management.
● Configured and managed synchronization to NTP Servers
● Scripted deployment of code
● Deployed and managed Splunk Agents (Universal Forwarders)

Education Management Corporation

Systems Administrator - Pittsburgh, PA
January 2013 to April 2016

● Responsible for availability and uptime of 500 servers
● Patch Management via SSCM & Red Hat Satellite
● Troubleshoot IIS & Apache web server.
● Monitor and manage system resources- Disk Space |CPU |Memory.
● Order and replace hardware failures (DIMMS Card, Hard disk, power supply)
● Set up Performance monitor counters for load testing.
● Troubleshoot unresponsive or sluggish website performance and implement solutions.
● Responsible for scheduling, monitoring, and implementing patching.
● Deploy, test, and verify new code and applications.
● Troubleshoot server performance via HP performance monitor, Task manager, event viewer & log files.
● Troubleshoot IIS & Apache web server.
● Monitor and manage system resources- Disk Space |CPU |Memory.

Education

MBA

University of Maryland, University College - Adelphi, MD
May 2009

BA in Economics

University of Maryland - College Park, MD
May 2004

Skills

- Onboarded logs via Universal Forwarder
- Certificate Management
- Built multi-site Splunk Clustered environment.
- Scripted Archiving Splunk frozen buckets to S3 Buckets
- Networking: Symantec Secure Access Cloud| Juniper Chassis | pfSense Firewall/router
- Splunk Team Lead (Gray Tier Technologies)
- On-Prem to AWS cloud migration
- Secure Remote: Putty| Remote Desktop Protocol (RDP) |Remote Desktop Manager| Integrated lights out (iLO)| iDrac| SSH port forward & X forwarding | XfreeRDP| Secure Access Cloud (SAC)
- Implemented Load balanced syslog Architecture in AWS
- Logical Volumes
- EC2
- Load Balancers
- Mitigating of Log4J on Splunk Servers
- Assessment of Customer environment to determine Splunk Architecture
- Assisted the Security Operations team to investigate data discrepancies.
- Implemented inbound and outbound network access via Security Groups
- Built Asset Reconciliation dashboard correlating Splunk data with CMDB.
- Cloud
- Server and port hardening via selinux (semanage)
- Migration: Splunk On-prem to on-prem migration | Splunk On-prem to AWS Cloud Migration
- Containers: Docker| Vagrant
- CloudTrail
- Route 52
- Led Splunk Migration effort to AWS 2023 instances.
- Wireshark, Symantec Secure Access Cloud (SAC)|Splunk Enterprise Security, Rapid 7
- Splunk Cloud Integration for multiple clients.
- Code Deploy
- IAM
- Built and configured Redundant firewall (pfSense)
- Interviewed and hired Splunk resources with Gray Tier Technologies
- Rapid7 to check and mitigate Server Vulnerabilities
- HEC
- SSM
- Implemented host-based firewall in Linux via firewalld
- Implementation of TLS certs for Splunk web and S2S communication
- Capacity planning to standup multi-site Clustered Environment
- Creating onboarding templates to streamline onboarding Use Cases Architecting| Builds
- Implemented third-party TLS certs to secure web communication.

- Create AWS Load Balancing for the Search Head Clustering
- Syslog
- AMIs
- Trained, hired, and developed new Splunk resources. Security Implementation
- Troubleshooting: Server performance | Website performance | Hardware failure | Application & Services
- Configuration Tools: System Center Configuration Manager (SCCM)| Red Hat Satellite| Ansible| Cluster SSH (CSSH)
- Recommended and implemented storage policy.
- EC2
- Consulting
- Security Groups
- Enabling FIPS on Splunk servers
- Enabled Security content for M-21-31 referencing Splunk security essentials.
- Certificate Manager
- Cloud: AWS Administration
- S3
- Scoping and Architectural reviews with customers
- EC2
- Enterprise Security. Rapid7, STIG Viewer
- ACM
- Security Tools
- Implemented Splunk SC4S Syslog solution.to ingest and parse Security Logs.
- Target Groups
- APIs
- Scripted Inputs
- Built a vSphere clustered environment with three ESXI servers.
- Implemented Splunk Connect for Syslog (SC4S) implementation for security appliances. Leadership
- Created AMIs for Splunk Components Recent Project Highlights
- S3 buckets
- Implemented Clustered Virtualized environment with 3 ESXI servers.
- Load Balancers
- Subscribed to AWS SnowBall Edge to migrate on-prem data to S3 buckets.
- Splunk Migration from On-Prem to AWS Cloud environment
- CodeCommit
- Splunk Migration from On-Prem to AWS Cloud environment.
- AMI
- Built Asset Reconciliation dashboard correlating Splunk data with CMDB. Tools & Applications
- Log Aggregation: Rsyslog | Syslog-NG | Syslog Connect for Splunk (SC4S)
- Automation: Bash Shell Scripting | Ansible| Git
- Load Balancing

- Cloud Trail
- DNS
- VMWare
- Active Directory
- Scripting
- TCP/IP
- DHCP
- Operating Systems
- Microsoft SQL Server
- System Administration
- Apache
- Authentication
- Azure

Certifications and Licenses

CompTIA Security+

ITIL Certification

RHCSA

Splunk Core Certified Power User
Present

Splunk Core Certified Consultant
Present

Splunk Cloud Certified Admin
Present

Splunk Enterprise Certified Architect
Present