SPLUNK ADMINISTRATOR SPLUNK ADMINISTRATOR SPLUNK ADMINISTRATOR - NDTI - HILL AIRFORCE, UT Clearfield, UT Work Experience SPLUNK ADMINISTRATOR NDTI - HILL AIRFORCE, UT January 2019 to Present   Experience in end-to-end event monitoring infrastructure of business-aligned applications.   Expertise in searching, monitoring, analyzing and visualizing Splunk logs.   Environment: Splunk 7.1, Splunk 7.3, Linux, Splunk Knowledge Objects.   Was an active team player, helped in fixing bugs and also carried out troubleshooting.   Analyzed security-based events, risks and reporting instances.   Troubleshooting of searches for performance issues by adding lookups, correct joints and using summary indexes.   Created Dashboards for various types of business users in the organization and worked on creating different Splunk Knowledge objects like, Calculated fields, Tags, Event Types, and Lookups.   Well versed on Parsing, Indexing, Searching concepts, Hot, Warm, Cold and Frozen bucketing.   Actively involved in troubleshooting issues.   Maintain documentation of applications including what work has been done, what is left to do and site-specific procedures documenting the Splunk environment.   Developed scripts to automate batch jobs, loading data into Splunk including syslog and log files.   Optimization of Splunk for peak performance by splitting Splunk indexing and search activities across different machines.   Involved in standardizing Splunk forwarder deployment, configuration, and maintenance across UNIX and Windows platforms.   Experience with eMASS, SIEM, Comparable tools and Using NESSUS to analyze Vulnerability Scans.   Work with a team of Information System Owners, Developers and System Engineers to select and Implement tailored controls in safeguarding system information.   Create Plans of Action and Milestones (POA&M) management for identifying vulnerabilities and performed compliance monitoring.   Experience with continuous monitoring of security controls and review of vulnerability scans and follow-up to ensure mitigations of vulnerabilities per standard operating procedures.   I develop root cause for weaknesses, resources requirements, remediation activities and project plan within required time for formal identification of weakness.   Conduct assessments of system safeguards and controls and respond to external audits as required.   Investigate, contain and report all Classified Message Incidents (CMIs).   Conduct vulnerability scans via the Assured Compliance Assessment Solution

(ACAS) for all assets on the AF network (i.e. work stations, server, switches, and routers). Conduct SCAP / STIG Viewer scans for STIG compliance checks on all applicable assets. Develop process and procedures for all day to day operations. IT Security Analyst Lumark Technologies, Inc September 2015 to December 2018 Installing and configuration Splunk multisite indexer cluster for data replication. Setting up Splunk Forwarders for new application tiers introduced into the environment and existing application. Responsible with Splunk Searching and Reporting modules, Knowledge Objects, Administration, Add-On's, Dashboards, Clustering and Forwarder Management. Splunk configuration that involves Saved search, summary search, and summary indexes. Experience with search ahead clustering and Index clustering. Experience with working on large datasets to generate insights and communicate insights to guide strategic roadmap. Extensive experience in setting up the Splunk to monitor the customer volume and track the customer activity. Installed and configured heavy, universal, and intermediate forwarders. Involved in Splunk upgradations, migrating infrastructure, troubleshooting Splunk Enterprise and capacity planning Analyzing reports generated by scanning tools and Providing recommendations on how to fix uncovered vulnerabilities Performing Web Application Scanning using WebInspect Proactively working in hosted SIEM environment to collaborate with engineers to detect and mitigate threats Creating a Plan of Action and Milestones and work accordingly to lower risk score across organization. Experience in analyzing results from vulnerability scanning and penetration testing in accordance with NIST 800-115, using tools like Nessus, WebInspect. Experience with FIPS 199/NIST 800-60 Standards for Security Categorization of Federal Information and Information system. Selecting the controls using NIST 800-53/FIPS 200, implementing controls and developing SSP and other key deliverable documents. Work with a team of Information System Owners, Developers and System Engineers to select and Implement tailored controls in safeguarding system information. Evaluating and/or creating System Security Plans (SSP), Contingency Disaster Recovery Plans (CDRP), Risk Assessment Reports (RAR), Security Assessment Reports (SAR) and Executive Summaries. Education Bachelor's in Cybersecurity University of Maryland - College Park, MD January 2018 to Present Bachelor's in Economics and

Management University of Yaounde 2 - Yaounde October 2008 to September 2012 Skills Nist, Splunk, Elasticsearch, Security, Ms project, Ms office, Documentation, Excel, Outlook, Powerpoint, Word, Linux (2 years) Military Service Branch: United States Army Rank: E4 Certifications/Licenses CEH November 2018 to November 2021 ComPTIA Security+ May 2018 to May 2021 AWS-Associate July 2018 to July 2021

Name: Jacqueline Bradford DDS

Email: lwilson@example.org

Phone: (810)599-9335