On-Site Service Specialist On-Site Service Specialist functioning as a Security Administrator - Operations Security Center Florissant, MO To obtain a position using my skills to be a senior level ArcSight Engineer. Work Experience On-Site Service Specialist Micro Focus April 2019 to Present Servicing the customer with specialised support for the product ArcSight and it's suite of tools. functioning as a Security Administrator Operations Security Center - St. Louis, MO October 2017 to Present Operations Security Center (NOSC), and Computer Network Defense Service Provider (CNDSP) functioning as a Security Administrator. ManTech International, ST. Louis, MO October 2017 - Present National Geospatial Intelligence Agency (NGA) ArcSight - Lead Engineer Micro Focus Arcsight Application Engineer that has eight years of enterprise level experience with hands-on troubleshooting and maintenance of ArcSight infrastructure, architectural designing, configuring, implementing, testing, and performance tuning enhancements for all of the ArcSight suite. These systems include: ESM, logger, smart connectors (Windows, Linux, and Sourcefire), load balancing connectors, event broker (Kafka), ESM/Logger forwarders, ArcMCs, and CONApps. Familiar with performing at a high level to meet service level agreements (SLA) and executing services within a fixed price, working in a performance-based environment where performance is based on predetermined Service Level Agreements or Acceptable Levels of Performance. Work performance is based on the customer Accepted Level of Performance. Sustains and maintains support in the development of all new onboarding programs with detailed documentation, and tracks progression of the procedures relevant to the task. Accustomed to constructing a pathway for data ingestion through one way transfer solutions between enclaves, such as data being ingested into an Elastic Stack for federal auditing regulations. Accomplishments: ? Determined and mitigated CORR database issues within current system and tuned certain trends and queries to have reports function properly and more quickly. ? Identified system misconfigurations and provided fix actions for better system performance and reduced outages by over 50% ? Implemented ArcSight data broker (Apache Kafka by Micro Focus) ? Implemented ArcSight Load Balancing connector in an HA pair to round robin over 25K EPS across 5 different RHEL servers hosting 10 syslog-ng connectors that fed in to a event broker for data subscriptions for ESM and Elastic infrastructure. ? Migrated old CONAPP appliances to use the new ArcMC (ArcSight Management Center) ? Tuned rules and data monitors to prevent excessive memory usage on existing system. ? Tuned queries and filters that fed trends that exceeded high amounts of table space by reducing the sizes down from over 400GB to around 20-30 GB while still having the required data fill the customers reports, best practice is to not have trends exceed 1GB but in some cases on larger networks, it's hard to prevent that. ? Designed new architecture for future growth to take advantage of the upcoming of ESMs new distributed correlation method and streamlining how the data gets from the source device to the ESM by reducing the amount of connectors needed while tuning map files to reduce stresss on certain connectors to prevent extreme data caching or service failure, plan is still in the works as the newest ESM release is only beta stages. ? Took current architecture and modified the CORR database to take full advantage of the 12TB from it's current 1TB outfitting while also implementing custom table spaces for each enclave and set custom retention periods for certain networks that didn't require data to be held as long as other classified enclaves. ArcSight - Engineer TEKSystems - Scott AFB, IL October 2016 to August 2017 Overall strategic mission in supporting the global and regional network defense centers data transport, normalization, parsing, and performance. Local responsibilities include: On-site SIM (Security Information Management) technologies, analysis, and engineering, and integration, support expert while examining and resolving operational issues. Design, test and deploy configurations for analysis and correlation content. Explain complex system capabilities to analysts and leadership Provide detection strategies and integration advice. Coordinate and collaborate with DISA Global program manager and engineers, global SIM embeds, and contracted system support organizations. Configure, patch, and upgrade Linux operating systems with Fusion I/O drives to meet operational needs. Conduct internal research to identify features, bugs, and resolution information. Develop and maintain software to transform external data into system-usable formats. Instruct local and customer personnel on network security and SIM related topics. Provide senior management with overall usage metric reports for all SIM technology. Accomplishments: ? Migrate from ArcSight ESM 6.5 to ESM 6.9.1 to 6.11 for over 25 ESM instances ? Stand up and configure ArcSight Management

Center server to control and configure connectors and loggers for within the enclave ? Stand up and configure ArcSight Logger solution within the multiple security stacks ? Building Acquisition portals in Data Orchestrator Linux SIEM Support - Administrator Northrop Grumman - St. Louis, MO October 2012 to October 2016 Overall strategic mission is supporting the global and regional network defense centers data transport, normalization, parsing, and performance. Local responsibilities include: On-site SIM (Security Information Management) technologies, analysis, and engineering, and integration, support expert while examining and resolving operational issues. Design, test and deploy configurations for analysis and correlation content. Explain complex system capabilities to analysts and leadership Provide detection strategies and integration advice. Coordinate and collaborate with DISA MA program manager and engineers, global SIM embeds, and contracted system support organizations. Configure, patch, and upgrade Linux operating systems with Fusion I/O drives to meet operational needs. Conduct internal research to identify features, bugs, and resolution information. Develop and maintain software to transform external data into system-usable formats. Maintain availability and functionality of cross-domain file transferring solution. Troubleshoot user issues related to file restrictions while using such cross-domain solution. Instruct local and customer personnel on network security and SIM related topics. Provide senior management with overall usage metric reports for all SIM technology. Accomplishments: ? Migrate from ArcSight ESM 5.2 to ESM 6.5. ? Stand up and configure ArcSight Management Center server to control remotely configured connectors for customers outside of the enclave ? Stand up and configure cross-domain file transferring solution for malware scanning, scrubbing and sanitizing of files before moving files over the enclave boundary ? Building Acquisition portals in Data Orchestrator Network Engineer Hewlett Packard Enterprise Services - Fort Knox, KY December 2010 to October 2012 Implemented, troubleshot and maintained enterprise network environments using multiple Cisco Nexus 7018's, 5020's, 2148's, Cisco Catalyst 3560 E's and Cisco 3110 Blade Enclosure Switches. Provisioned virtual switches (VDCs) and associated resources, managed IP space, and utilized Netscout and Infinistream traffic capture/sniffing devices while using Red Hat Linux terminal and Raritan KVM devices. Set up and maintained SYSLOG and

SNMP monitoring and control environments. Developed documentation for performance monitoring of network assets for the HQ US Army Human Resources Command to support the entire Army. Accomplishments: ? Worked with numerous remote sites to troubleshoot connectivity for the migration of the entire US Army software portfolio; consisting of 200+ software suites comprising of over 500 local servers and tens of thousands of end point users. ? Configured F5 to add/remove servers/members from the pool. ? Provided assistance to the Network Enterprise Center (NEC) on replacing 216 line cards for Brocade Fastiron SX 1600 devices throughout the entire campus at Human Resources Command for both Data and Voice Over IP (VOIP) networks. SYSTEMS SUMMARY TECHNICAL TRAINING: HP ArcSight Certified Integrator Administrator (40 hrs.), RHEL (40 hrs.), TCP/IP (10 hrs.), CERT SEI Pipeline V5 (16 hrs.), Snort Intrusion Detection System (30 hrs.), WinDump/TCPDump (5 hrs.), Oracle 11g (10 hrs.), Microsoft Visual Studio (100 hrs.), McAfee HBSS (10 hrs.), NetScout InfiniStream (10 hrs.), WireShark (10 hrs.), Nessus Scanner (40 hrs.), Splunk (5 hrs.), Bro IDS (5 hrs.), OSSIM, OSSEC, Alien Vault USM, Security Onion, Dell and HP Enterprise Hardware. Programming Languages: Java, HTML, PHP, and BASIC. Education Management Information Systems St. Charles Community College - Cottleville, MO Skills Cyber Security, Information Security, Linux, Siem Certifications/Licenses Driver's License Additional Information SKILLS ? Problem solver ? Self-motivated worker ? Adaptive team player ? Extremely communicative

Name: Daniel Smith

Email: carol36@example.net

Phone: (677)864-5848x58771