David Anderson

Herndon, VA 20171

(202) 780-6951

David@misplaced.us

EDUCATION

B.S.B.A. in Computer Information Systems
Northern Arizona University, Flagstaff, AZ
Certificate: System Administration and Security

EMPLOYMENT HISTORY

Integration and Operations Support Lead
CDM Phase 3 (DEFEND) – Task Order 2 Bravo, 2 Delta, 2017 – *(current)*
Booz Allen Hamilton; McLean, VA

- Lead and grow a team of Integration Leads and that manage the integration and implementation of unique custom technical solutions across 34 Federal Government agencies, sub-agencies, and operational divisions.
- Manage a team of 30-40 FTEs responsible for the implementation of new solutions and existing CDM Phase 1 and Phase 2 implementations.
- Provide guidance and input to the design of unique, custom, multi-tool technical solutions to solve complex problems across the government space to include production of basis-of-estimates, proposal language, and staffing.
- Provide technical mentorship and guidance to engineers, as well as leadership development to forward-facing Leads with a focus on customer engagement, expectations management, and cross-workstream communication.
- Continued management of Splunk Deployment Team to include process creation and leadership of scheduled deployments, upgrades, operational support, and service requests of the CDM Solution.
- Lead an engineering team to build custom, innovative solutions to streamline lengthy processes, alleviate pain points, and reduce LoE for common tasks by building custom Splunk Apps and technical add-ons, as well as ansible automation playbooks.

Splunk Deployment Lead
CDM Phase 1 – Task Order 2 Bravo, 2 Delta, 2016 – 2017
Take2 Consulting LLC, Subbed to Booz Allen Hamilton; McLean, VA

- Managed a team of Splunk Subject Matter Experts to deploy and maintain 34 separate instances of a multi-tier Splunk implementation across 90% of the Federal Government space.
- Provided technical mentorship and guidance in hardware sizing, licensing, architectural design, and implementation of a custom, complex solution.
- Built a team from two engineers up to thirteen SMEs supporting Integration and Operational support across 34 implementations in over 100 sites.

- Lead operations in monitoring and maintaining data feeds and mapping of Hardware Asset Management (HWAM), Software Asset Management (SWAM), Configuration Settings Management (CSM), and Vulnerability Management (VULN) data from sensor-level components all the way up to dashboard-level systems.
- Facilitated communications by serving as a point of contact between technical customer and engineering all across all 34 agencies.
- Represented Splunk Deployment Team directly when communicating with both customer and program leadership.

Splunk Subject Matter Expert, Data Manager
CDM Phase 1 – Task Order 2A, 2015 – 2016
Defense Point Security, Subbed to ManTech International; Herndon, VA

- Perform Architectural Design, Sizing, Development, and Deployment for Splunk to be spread across 13 different components of DHS.
- Design, create, and manage technical integrations between McAfee ePO (and related tools), BeyondTrust BeyondInsight (including Retina), ForeScout CounterACT, and RSA Archer.
- Map, plan, organize, and maintain Hardware Asset Management (HWAM) data, Software Asset Management (SWAM) data, Configuration Settings Management (CSM) data, and Vulnerability Management (VULN) data from sensor-level components all the way up to dashboard-level systems.
- Serve as a Subject Matter Expert for communication between team mates and customers, both technical and non-technical.
- Provide technical advice and problem-solving assistance in general as a technical leader on the project.

Information Security Analyst – Senior, 2013 – 2015
Northern Arizona University; Flagstaff, AZ

- Performed auditing, documentation, reporting, and review of threats and vulnerabilities, to include executing remote and on-site vulnerability scans of data networks and computing devices using.
- Provided incident response and remediation support as a permanent member of the Computer Security Incident Response Team.
- Provided technical advice, problem-solving assistance, and answers to questions regarding security program standards and procedures.
- Participated in the network system architecture, design, and capacity planning for new products and technologies associated with information security.

Software Systems Assistant Engineer – Web Security, 2010 – 2013
Northern Arizona University; Flagstaff, AZ

- Maintained web servers for the university with a focus on web security with mind to OWASP Top Ten, especially Injection Vulnerabilities.
- Aided faculty in migrating and securing websites, applications, and servers.
- Tested and patched servers for security vulnerabilities.
- Programmed unique solutions for different problems on a weekly basis.

TECHNICAL SKILLSETS

Splunk – 5 years experience

- **Splunk Enterprise**: Multi-tiered, Deployment Server, SH Clustering, Indexer Replication, HTTP Event Collector, SSO Integration

- **Data Modeling, Performance Tuning, and SPL:** *CIM Compliance, Summary Indexing, Content Development, and a Solid handle on Splunk Query Language.*

- **Core and Third Party Splunk Apps** Including Enterprise Security, DB Connect Windows/AD integrations, Tenable and other COTS tools.

- **Custom Integrations**: *Custom applications, System Messages, Messaging Queues, Undocumented REST APIs, and more.*

Systems Administration

- **Red Hat Enterprise Linux and CentOS** – 8 Years
- **Apache and nginx Webservers** – 8 Years

Development

- **Unix Shell** – 8 Years
- **PHP: 4 & 5** – 5 Years
- **Python: 3.x & Django** – 4 Years
- **Ansible & Terraform** – 3 Year

Cloud Infrastructure and Automation

- **Amazon AWS EC2:** *EC2 Instances, AMIs, VPC structures, RDS, Route53 DNS, S3 Storage and Complex IAM Roles* – 5 Years

- **Ansible Automation:** *Experience using and developing in Ansible for automated deployments and system management* – 3 Years

- **Terraform Automation:** *Experience using and developing in Terraform for infrastructure management and customization* – 3 Years

Potpourri

- Certified Splunk Architect
- Red Hat 7 Certified Systems Administrator (RHCSA)
- Active Clearance info available upon request