**David Coleman**

**Objective:**

Locate a challenging position that utilizes my experience, knowledge and leadership abilities while creating opportunities for long-term professional growth and continued success.

**Security Clearance: “Active** **Top** **Secret** “

**Technical Skills:**

* Operating Systems: Windows, Linux
* Microsoft tools: Microsoft office suite
* Process/ Standard: FISMA, Vulnerability Management NIST SP 800-37, Security Risk Assessment/Security Attestation – NIST

SP 800-53, FIPS, (C&A) Certification & Accreditation, A&A Authorization & Accounting (RMF) Risk Management Framework

* DNS, VPN, Websense, SolarWinds (LEM)
* Virtual machines, Log analysis, Malware analysis, Customer service skills, Vulnerability scanning, and Patching of systems
* Splunk, Remedy, STIG, FireEye, Sourcefire Tenable, Nmap, and Mfilt (Sonicwall).
* SWOT analysis, Risk analysis, and User Acceptance Testing (UAT)
* Vulnerability scans using Websense, Nessus, vulnerability management, manage intrusion alerts, and other intrusion detection software tools

**Employment:**

**22nd Century ISSO**

**April 2021 to present**

* Reviewed ACAS scans daily for vulnerabilities in systems I managed
* Uploaded ACAS scans into VRAM weekly
* Ensured all devices are uploaded and show in asset group
* Used eMass to manage systems. Update expiring POAMS and complete self assessment on controls.
* Review DADMS application as well to manage SW/HW list/ Customer assets
* Used HEAT ticket system to fix or track issues
* Used TEAMS application for meetings and training
* Continues monitoring on all step 6 systems as well

**(RMC) Resource Management Concepts (ISSO)**

**Patuxent River Maryland**

**July 2020 to April 2021**

* Collect all documentation and artifacts needed to send to step 4 for an ATO
* All systems I worked were in a SAP environment
* Weekly meetings with customer to ensure assessment was on track to meet deadline
* Traveled onsite to customer if needed to have eyes on validation
* Reviewed SSP, SCTM, SAP, to get a deep knowledge of systems
* Helped customer with completing any documentation they did not have full understanding of
* eMASS tracking for all unclassified systems
* ACAS scan to track vulnerabilities and present to customer for patching
* Reviewed hardware and software list for any package
* Looked over network diagrams to make sure everything was captured in their boundary
* Reviewed STIG’s and SCAP scans
* Write memos to the PSO for approval of software and hardware
* Worked closely with V&V to get them an ATO
* Also worked IATT’s as well

**JSP/BOOZ ALLEN**

**KFORCE: Security Control Assessor (SCA)**

**October 2019 February 2021**

Crystal City VA.

* Plan and attend kick off meetings
* Assess and validate packages in the step 4 process
* Work closely with ISSO’s from steps 1-6
* Use eMass to validate controls and collect artifacts
* Update and correct templates if needed SAP/SAR etc.
* Prepare escalations for expired systems
* Assess vulnerability scans from ACAS
* See packages all the way to an ATO.
* Create, review, and provide various reports and briefing materials.
* Communicate matters to personnel at all levels and build and maintain organizational relationships to ensure awareness and effective messaging.
* Execute word processing and data entry, including demonstrating expertise and
* Establish and maintain records and files, including properly marking and disseminating materials in accordance with law, regulation and policy, and performing appropriate reductions in accordance with general records schedules.

**SimVentions:** Fredericksburg VA.

Information Assurance Specialist

Feb. 2018 to August 2018

* Review system packages through eMass to convert from DIACAP to RMF
* Do annual and quarterly reviews on packages as well as RBC
* Use ACAS software to run vulnerability scans
* Can do RMF steps 1-6 but mostly steps 2 and 3 here
* Use FMATS to review compliant and non-compliant STIGS
* Build SAP’s as well as assist system owners with any documentation they need to be compliant

**PRISM:** Rosslyn VA.

Security Assessor

December- 2016 to Feb. 2018

Analyzing systems for the Department of State and other agencies, which include

* Document findings based on NIST, FISMA, and FIPS controls
* Responsible for Assessment and Authorization
* Review POAM closure forms and document in IVVA form
* Review and log cases in Remedy ticket system
* Write all case analysis based on failed controls and decide weather system can be provided an ATO
* Also. Do an internal QA process, to make sure all documentation is correct

**ALION Science & Technology: Lanham MD.**

**October 2009 – December 2016**

**Information Assurance Analyst**

October 2014 – December 2016

* Ability to perform gap analysis and able to help with best practice recommendations
* Written security documentation
* Wrote papers on the way PKI, and Symmetric encryption work for our Deputy CISO
* Update company security website weekly with security articles
* Offer best practice recommendations for FIPS standards and other 800- series standards
* Analyze DNS logs daily
* Pull malicious URL’s to be analyzed, filtered out and blocked
* Test Malware samples in a Sandbox environment. Use Wireshark, Process Explorer, Install rite, and other various tools
* Monitor user usages and applications Phone Factor/VPN/Microsoft Azure/ and Two Factor Authentication
* Add and remove filters in the LEM {Log Event Manager} as necessary
* Use Websense to add and remove Malicious URL’s, monitor band with, and filter out bad websites daily for the whole enterprise
* Run weekly reports in Websense as well to find vulnerabilities in the enterprise
* Build and run cables in server room for new and old Appliances
* Act as a tier two helpdesk for tier one as needed
* Provide analysis and monitoring with Source Fire and Snort on as needed basis
* Use the Ghost application to image machines that come to our location with any type of infection
* Worked with stakeholders in the setup of VPN for remote locations
* Clean systems of malware remotely if needed
* Sit in with CISO to assist with NIST SP 800-53. To associate a group with each section in documentation for compliance
* Attend all Patch meetings
* Wrote all documentation for the implementation of Nessus vulnerability scans. Which include: Project plan, Procedures, Task document, memo to company, and FAQ document
* Forensically acquire digital evidence and examine data pertaining to OIS investigative actions, including following legal and policy requirements and presenting findings as necessary during administrative and criminal court proceedings, and briefings.
* Support data management and processing requests.
* Perform testing of computer hardware and software.
* Research computer science-related policies and protocols, conduct necessary benchmarking, and develop or refine procedures for assessing the effectiveness of data processing processes.
* Create, review, and provide various reports and briefing materials.
* Communicate matters to personnel at all levels and build and maintain organizational relationships to ensure awareness and effective messaging.

**Jr. Information Security Analyst**

November 2012 – September 2014

* Shadow senior security members to gain understanding of Source Fire, Websense, Snort IDS/IPS, Solar winds LEM
* Analyze VPN logs phone factor, Microsoft Azure and DNS entries
* Build Network cables for server room
* Consult on new technologies
* Understanding of NIST 800-53 to ensure system compliance
* Monitor Checkpoint Firewall
* Experience with SonicWall mail filter and Netwitness

**Helpdesk/Desktop Support**

October 2009 – October 2012

* Build and Run Ethernet cables for our Servers, Routers, and Switches
* Provide help desk and desktop support for end users
* Experience resolving VPN, password, and Outlook issues
* Used Virtual machines, Remote desktop a Sandbox, GFI Languard, and Tenable.
* Analyze DNS logs to find Malware, Spyware, Bots/Beacons, scripts, (etc.)
* Ghost hard drives to further investigate present malware
* Apply patches to the Enterprise system and ensure reliability of patches
* Provided help with Blackberry, Apple, and Android issues
* Fix and install printers as needed
* Remove and install hard drives, memory, and RAM if needed
* Install and wipe operating systems
* Add or remove users from Active Directory
* Restore passwords for locked out users
* Assisted with power point presentations
* Used Manage Engine ticket system to log and keep records of user’s issues
* Help users with the installation of new applications or hardware
* Remote desktop into user’s computer if needed

**Education**

* College of Southern Maryland
* Learning Tree: System and Network Security Introduction; Introduction to Networking; Network configuration and troubleshooting
* ALION Science & Technology: Cyber Warrior training

**Certifications:**

* Security+ (Certified)