Jay Davis, *CISM*

Richardson, TX 75044 Mobile: (703) 915-8659
Jay49davis@hotmail.com https://www.linkedin.com/in/Jay-Davis

Enterprise Solutions | Systems Cyber Security Engineer and Leader

A 20+ year experienced technology leader and mentor with extensive systems and security experience in both the public and-private sectors. Expertise in leading Governance, Risk and Compliance (GRC) teams for Enterprise Solutions through Enterprise & Information Risk Management, Policies and Standards creation, Vulnerability Management, Identity Access Management and IT Auditing. In-depth knowledge of multiple Security Standards (NIST, SOC, PCI-DSS, etc.).

Currently finishing a Bachelor of Science Degree in Cybersecurity and Information Assurance, while preparing for the CISSP certification. Maintained a DoD Security Clearance from 2002 to 2015 when the clearance was archived due to lack of activity.

Key Career Accomplishments/Achievements

- Meeting PCI-DSS requirements by leading the teams responsible for resolving, remediating, mitigating and/or establishing compensating controls for over 7,500 Pen Test vulnerabilities, within 19 days, allowing the organization to regain their Attestation of Compliance (AOC) by providing a clean Pen test.
- For a bi-annual auditing process to establish the Authority to Operate (ATO), consistently, for a three-year period, led teams to provide evidence for over 100,000 individual settings, in less than a two week period, based on NIST 800-53 Configuration Management controls as defined by multiple Secure Technical Implementation Guide's (STIG's).
- Reduced vulnerabilities from over 60,000 non-compliant configuration (CM-6) findings to zero for environments involving servers/workstations in multiple OS's (application, middleware or infrastructure) in an enterprise structure of four locations, over 11,000 employee's serving 21.5 million people.
- Managed, led and mentored 16-member Service Desk team, providing multiple tier level support and resolving all feasible technical issues.
- Certified Information Security Manager (CISM), *other certifications listed at the end of this document*

Career Progression

Irvine Technology Corporation | Alorica

Global Cyber Security Engineer, *Dallas, TX* *11/2018 – 03/2019*

Alorica is the nation's leading provider of outsourced communications solutions, a global organization with over 100,000 employees, spanning 36 countries.

Member of the Information Security team specializing in Architecture and Governance, Risk and Compliance. Project technical / team lead for the PCI-DSS re-certification of the AOC/ROC.

- Resolved, remediated, mitigated and established compensating controls for 7,500+ Pen Test vulnerabilities which allowed the organization to regain their AOC (Attestation of Compliance) by providing a clean Penetration Test.
- Developed successful SOC 2 Type 1 (documentation of procedures and controls) and SOC 2 Type 2 (evidentiary proof of procedures and controls) compliance reports for Data Center environments required by American Express resulting in cessation of multiple imposed fines.
- Created Qualys PCI DSS scanning process and procedure for SOC remediation by severity.
- Led the corporate posture (with one other engineer) for Identity Access Management (IAM), Mobile Device Management (MDM) Mobile Application Management (MAM), Single Sign On (SSO), Self Service Password Reset (SSPR) solutions to be fulfilled through a third-party vendor.
- Created the procedures for the Security Operation Center (SOC) to categorize and prioritize findings and then implement necessary remediation processes and escalation procedures.
- Forged long-term strategic relationships with the teams responsible for remediation and the managerial escalation paths in order to budget time and essential resources for remediation.

TM Floyd & Company | Blue Cross Blue Shield of SC
Sr. IS Cyber Security Engineer, *Dallas, TX* *03/2015 – 06/2018*

TM Floyd is a contracting agency whose customer was is Blue Cross Blue Shield of South Carolina an enterprise structure of over 11,ooo employee's serving 21.5 million people.

Creator, Leader, and Mentor of the Operational Systems Compliance *(OSC)* Team – effectively training and mentoring OSC staff to enable effective Information Assurance (IA) practices – in accordance with corporate GRC standards through Defense Information Systems Agency (DISA) Secure Technical Implementation Guide (STIG), National Institute Of Standards and Technologies (NIST) 800-53, ISO 9001:2015 and organizational Risk Management Framework (RMF) requirements.

- Before the OSC's team assumption of daily vulnerability scans tasking, the organization faced over 60,000 non-compliant CM-6 findings. During the OSC's tenure, there were zero non-compliant findings for Windows, VMware or HyperV environments involving servers (application, middleware or infrastructure) or workstations, Group Policy or Active Directory.
- Encouraged internal operations teams to focus on vulnerability assessments and remediation/mitigation techniques across multiple platforms for the application, middleware and infrastructure owners, achieving 40% reduction in non-compliant vulnerabilities.
- Created security documentation for the implementation of Organizational Compliance standards: Policies; Standards; Guidelines and Work Instructions, allowing for Enterprise Risk Management implementation.
- Provided Windows/Virtual environment vulnerability mitigation and remediation for patching, upgrades and configurations through Group Policy, Active Directory and Registry changes for Change Management compliance.
- Compiled configuration evidence in the form of screenshots, configuration scripts, and created documentation such as Business Risk Justification's, Functional Policies and/or POAMs as prepared artifacts, system security plans, security controls traceability matrix, and security concept of operations, to support the Authority to Operate *(ATO).*

General Dynamics Information Technology | PACOM
Sr. System Engineer / Administrator, *Oahu, HI* *07/2012 – 03/2015*

- Created, provisioned, and maintained enterprise-level servers and workstations for multiple world-wide classified networks for Department of Defense (DoD) in Pacific Command (PACOM) achieving NIST 800-53 compliance.
- Developed an Endpoint Protection solution for local and remote based "Top Secret" networks (located in governments with information sharing agreements with United States) – servers and workstations where semantic Endpoint Protection (SEP) was utilized and updates occurred through air-gapping definitions.

General Dynamics Information Technology | USACE
Sr. System Engineer / Administrator | IANO, *Kabul, Afghanistan* *02/2011 – 06/2012*

Served as Information Assurance Security Officer (IASO) and Sr. Systems Engineer / Administrator in virtual and physical Enterprise environments in the Northern Afghanistan Region.

- Leader / Mentor of a 16-member Enterprise Service Technologists, providing Tier I, II, and III support, resolving all feasible technical issues.
- Developed "Data-At-Rest" encryption solution for Northern Afghanistan region using Trend Micro's "Mobile Armor" encrypting USACE workstations. Refined solutions by instituting Bit Locker across the region.
- Developed back-up and Disaster Recovery solution utilizing Symantec BackUp Exec for northern Afghanistan's 8 regional, 1 headquarters and 1 HQ back up locations. Managed through one BackUp Exec Administration Console for disk to disk, disk to tape, grandfather to father to son rotation methodology for backup media in which there are three or more backup cycles, such as daily, weekly and monthly.

Lockheed Martin | DoJ
Sr. System Administrator, Level IV, *Washington, D.C* *10/2010 – 02/2011*

- Revised Security Framework from NIST 800-53 rev 3 to rev 4 version.
- Upgraded the Disaster Recovery System and Backup/Archiving solution to the current version of Symantec.

Applied Computing Technologies | FEMA
System Administrator, *Washington, D.C.* *08/2009 – 08/2010*

General Dynamics Information Technology | DBSP
Windows/Linux System Administrator, *Continental United States* *06/2004 – 07/2009*

General Dynamics Information Technology | DoN HR
Web Master / System Administrator, *San Antonio, TX* *03/2002 – 05/2004*

Education

- Western Governors University – currently enrolled, completing the final years of Bachelor's Degree. Course of Study - Cybersecurity and Information Assurance
- Pursuing CISSP training and certification

Community Involvement

CSA Cloud Alliance, Information Systems Security Association (ISSA), Information Systems Audit and Control Association (ISACA), International Information Systems Security Certification Consortium (ISC2).

Technical / Software

Operating Systems & Servers:

Windows (XP/7/10), Windows Server (2003/2008/2012/2016), VMware (4.0/5.0/5.5/6.0) VMware vCenter, (ESX, ESXi, Hyper-V Hypervisors), Red Hat Enterprise Linux (RHEL), Windows Internet Information Server (IIS), Windows Server Update Services (WSUS)

System Security Assessments/Hardening Tools:

Nessus, Tripwire, Qualys, MITRE, CVSS, STIG Viewer, Active Directory/Group Policy, Symantec Endpoint Protection/ Backup Exec, KACE, SANS 20 Critical Security Controls, Certificate Services - Public Key Infrastructure (PKI)

Key Processes:

Change Management, Incident Management, Endpoint Protection, Vulnerability Assessment, Remediation and Mitigation, Security Documentation, ICMP, DHCP, DNS, HTTP, FTP, VPN, DNSSec

Architectural Tools:

CSA Cloud Control Matrix (CCM), CSA Consensus Assessments Initiative Questionnaire (CAIQ), CSA Star Registry, European Network and Information Security Agency (ENISA) Cloud Computing and Risk Assessment

Certifications

Certified Information Security Manager (CISM) *(Certification # 1840465)*

Certificate of Cloud Security Knowledge (CCSK) *(Code: 5gcoMUtyn7Zc4oe7zAaRVwiQ)*

Microsoft Certified Solutions Associate (MCSA) Windows Server 2012 *(Certification # F018-5583)*

VMware Certified Professional (VCP5-DCV) *(Code: 11374564-91D1-97DC9ED1B49B)*

Certified Identity and Access Manager (CIAM) *(Certification # 4239)*

Certified Access Management Specialist (CAMS) *(Certification # 4238)*

Microsoft Certified Technology Specialist (MCTS) Windows 7 *(Certification # A762-8759)*

Microsoft Certified Professional (MCP) Windows *(Certification # E546-4143)*

Microsoft Specialist (MCTS) Windows 7 *(Certification # F4969530)*

CompTIA Security +; A +; Network +