DEVIN MAYO

Mayodevin@gmail.com

202.280.3769

**PROFESSIONAL SUMMARY**



Over 19 years of experience in Information Technology services supporting security initiatives for government and commercial clients.

Work experience encompasses threat analysis, Vulnerability Development, reverse engineering, threat hunting incident response, Vulnerability assessments, network surveillance, Risk Management Framework (RMF), National Institute of Technology (NIST), System Development Life Cycle (SDLC), Information security documents, developing and promulgating Security Assessment Plans (SAP) and Security Assessment Reports (SARs), Controlled Unclassified Information (CUI), Governance Risk and Compliance (GRC), Pentesting, Red team

 **EDUCATION AND CERTIFICATION**

**St. John’s University**

**BA of Science, Business Management**

Certified Authorization Professional CAP In-Progress

Security +

Able to Obtain Clearance

**PROFESSIONAL EXPERIENCE**



**Options Clearing Corporation 3/2022-5/2023**

**Sr. ITCyber Security Architect/ Analyst**

* Conducted 3rd party risk assessments on vendors before their solutions were onboarded into our production environment.
* Assessed Application security code vulnerabilities in Jira, and Black duck and reported to Executives weekly in order to provide insight into existing code risk that matched CWE vulnerabilities
* Lead the Security Observation Risk Tracking within Service Now to track organizational risk reported

from all departments and quarterly red team tests, and security reports.

* Conducted quarterly Special Risk assessments that were reported to executives to highlight specific risks within the organization and how we can address them
* Ran Daily stand up meetings for Cyber Risk team to organize daily tasks and prioritize team objectives.
* Performed Asset Accreditation for Windows and Linux servers that were going into production and development environments
* Conducted web application security testing using tools like OWASP ZAP and performed manual testing to identify vulnerabilities like SQL injection and cross-site scripting (XSS).
* Conducted social engineering and physical security testing to assess the effectiveness of the clients security controls.
* Analyzed malware and performed reverse engineering to understand its behavior and identify the attacker intent.
* Prepared detailed reports and documentation of the testing process, vulnerabilities identified, and recommendations for remediation.
* Communicated findings and recommendations to executives and collaborated with them to improve the overall security posture.
* Conducted in-depth analysis of complex binary files using Ghidra and IDA Pro to identify potential vulnerabilities and reverse engineer malware.

**Coastal International 2/2012-3/2022**

**Sr. IT Security Analyst**

* Provided support and developed systems to manage, research, and enhance effectiveness of vulnerability technology
* Reverse engineered source code for testing, software integration and documenting the finding to provide lifecycle maintenance
* Developed scripts and Playbooks to automate configuration management vulnerability detection and containment within the AWS Cloud security and compliance suite
* Developed Vulnerability assessment to test existing environments according to security benchmarks
* Created daily routines that focused on Risk assessment, vulnerability scans, security and security audits to identify, document, assess, and remediate risk in order to control gaps and vulnerabilities
* Managed and lead effort to successfully achieve ATO within Multiple Cybersecurity frameworks within a hybrid Cloud Architecture and pure cloud environments (FedRamp, NIST, HITRUST, NIST CSF, ISO 27001)
* Develop training on best practices for developing secure software and hardware configuration management within a cloud environment
* Created security policies for AWS instances of critical security metrics to provide insight about the operational status to senior leadership
* Utilized hands on reverse engineering tools to gain deeper insight into Vulnerabilities (IDA Pro, Ghidra, Binary Ninja)
* Deployed, automated, managed and maintained AWS compliance for cloud solutions.
* Provide daily leadership to A&A and Incident response team in order to cultivate a mature security process responsible to ensure program development, project planning, vulnerability management, gap analysis and assigning systems and tasks to A&A team daily
* Oversaw HIPAA training in order to heighten the importance of protecting individual’s information as it traverses the information system.
* Developed Security Assessment Report (SAR) in the completion of the Security Test and Evaluation (ST&E) questionnaire using NIST SP 800-53A required to maintain Company Authorization To Operate (ATO), the Risk Assessment, System Security Plans, and System Categorization.
* Led effort to implement a new enterprise SIEM tool that created alerts and provided detail analyses of network activity
* Created Information resource to highlight Information Security best practices and the policy and procedures in place for the maturing of the organization's security posture.
* Led training efforts to connect appropriate security controls with security alert information for Federal Information System based on NIST 800-37 rev1, SP 800-53, FIPS 199, FIPS 200, and NIST SP 800-53A R4
* Conducted daily IT risk assessment within the DOD (Army) to identify system threats, vulnerabilities and risk, and generate reports to present to stakeholders in an effort to raise security awareness organization wide
* Developed training for department in order resolve PIV card administration issues within US Access, which led to enhanced user experience
* Led deployment of USAccess and led Kickoff meetings, with all necessary project teams’ as well as daily/weekly calibration meetings in order to test equipment, track key participation and review rollout experience with stakeholders
* Manage and coordinate deployment and training rollouts of PIV enrollment and issuance
* Continuously providing technical knowledge in computer network theory, IT standards and protocols, as well as sharing knowledge about the lifecycle of cyberspace threats, attack vectors, and methods of exploitation to stakeholders and the cybersecurity team within the DOD Army.
* Maintained daily, review and update of information security system documentations, including System Security Plan (SSP), Plan of Action & Milestone (POA&M), Risk Assessment (RA), policies and procedures, security control baselines in accordance with NIST guideline and security practices.
* Provide daily guidance to stakeholders to assess security controls and develop security assessment report (SAR)
* Develop vulnerability reports and dashboards, for incident response teams in order to provide new insight into existing vulnerabilities.
* Worked with vulnerability scanning tool support engineers to identify, troubleshoot, and remediate issues on a daily basis.
* Provide process improvement recommendations for day-to-day operations and give technical guidance to the Risk Management Team and other stakeholders on a daily basis.
* Provide support to the Incident Response and Investigation Teams when called upon.
* Provides daily details to guide A&A activities (Categorize, Selection, Implement, Assessment, Authorize, Monitor) according to the A&A project plan.
* Perform vulnerability assessment scans on a daily basis within host based operating systems, Web Applications, and Code reviews to perform analysis of scan results
* Perform daily analysis of scan results to determine applicability on a daily basis.
* Review authorization documentation for completeness and accuracy for compliance.
* Facilitate Security Control Assessment (SCA) and Vulnerability management activities.
* Executed examine, interview, and test procedures in accordance with NIST SP 800-53A Revision 4.
* Ensure cyber security policies are adhered to and that required controls are implemented.
* Validated information system security plans to ensure NIST control requirements are met.
* Assist team members with proper artifact collection and detail to client’s examples of artifacts that will satisfy assessment requirements.
* Review security logs to ensure compliance with policies and procedures and identify potential anomalies.
* Update and review A&A Packages to include Core Docs, Policy & Procedures, Operations and Maintenance Artifacts, SSP, SAR, FIPS 200, FIPS 199, and POA&M.

 **Cyber Point Baltimore, MD 10/2007– 2/2012**

 **Information Security Analyst**

* Ensure proper system categorization using NIST 800-60 and FIPS 199; implement appropriate security controls for information system based on NIST 800-53 rev 4 and FIPS 200.
* Conduct security assessment interviews to determine the Security posture of the System and to
* Perform kick Off Meetings
* Apply appropriate information security control for Federal Information system based on NIST 800-37 Rev 1.
* Facilitate Security Control Assessment (SCA) and monitor activities.
* Developed Security Assessment Report (SAR) in the completion of the Security Test and Evaluation (ST&E) questionnaire using NIST SP 800-53A required to maintain Company Authorization To Operate (ATO), the Risk Assessment, System Security Plans, and System Categorization.
* Reviewing, maintaining, and ensuring all assessment and authorization (A&A) documentation is included in the system security package.
* Perform information security risk assessments and assist with the internal auditing of information security processes. Assessed threats, risks, and vulnerabilities from emerging security issues and also identified mitigation requirements.
* Work with system owners to develop, test, and train on contingency plans and incident response plans.
* Tests, assess, and document security control effectiveness. Collect evidence, interview personnel, and examine records to evaluate effectiveness of controls.
* Review and update remediation on plan of action and milestones (POA&Ms), in organization’s CSAM Work with system administrators to resolve POA&Ms, gathering artifacts and creating mitigation memos, residual risk memos and corrective action plans to assist in the closure of the POA&M.

**COMPUTER & SOFTWARE PROFICIENCIES**

⬥ Microsoft Office Suite

⬥ Incident Response

⬥ Linux/Android Kernel

⬥ Vulnerability Assessment developer

⬥ Credential/Identity & Access Management

⬥ Homeland Security Presidential Directive 12 (HSPD-12)

⬥ FIPS 201-2

⬥ DoD cybersecurity experience

⬥ Experience with DoD military health

⬥ Experience with DoD IAVM (Information Assurance Vulnerability Management) Program

⬥ Security +

⬥ Reverse Engineering

⬥ ACAS/NESSUS, SCAP

⬥ Fedramp

⬥ Azure Global Administrator

⬥ Azure Active Directory Engineer/Admin

⬥ Linux

⬥ Active Directory Global Administrator

⬥ Sharepoint Global Administrator

⬥ Powerpoint

⬥ CSAM

⬥ Adobe

⬥ NSAT

⬥ ARCHER

⬥ Nessus Vulnerability Scanner (SC-5)

⬥ Splunk

⬥ MS Project