

Security Specialist Security Specialist Security Specialist - Akira Technologies Inc Beltsville, MD A dedicated Cyber Security Analyst with 5 years+ experience in RMF and over 10 years+ of IT experience seeking a position where attention to detail and devotion to customer satisfaction is crucial. Possess an excellent ability to work in a team environment and willingness to acquire new skills.

FIVE YEARS INFOSEC SKILLS SUMMARY

- ? Experienced in creating, reviewing and updating security documents.
- ? Working knowledge of NIST 800-53, NIST RMF, FIPS and FISMA dedicated guidelines to comply with federal and private agencies
- ? Perform categorization of information system using FIPS 199 as a guide or its equivalent NIST SP 800-60.
- ? Possess in-depth ability performing information security risk assessments and analysis, risk mitigation in large-scale networked application environments
- ? Supporting client with POA&M evaluation as part of remediation process
- ? Support client with creating memos and SOPs for system security controls
- ? Experienced working with NIST SP 800-53 rev 3 and rev 4
- ? Knowledge of IT security architecture (firewalls, Intrusion Detection Systems, Virtual Private Networking, and virus protection technologies
- ? Excellent analytical and problem-solving skills as well as inter-personal skills in interacting with team members, clients and top management as well
- ? Ability to work under difficult terrain and meet deadlines in required time frames
- ? Excellent verbal and written communication skills
- ? Collaborate with other information security and IT team members to develop and implement innovative strategies for monitoring and preventing attacks
- ? Cloud security knowledge with experience in FedRAMP systems
- ? Experience supporting cloud system integrator interconnected with other external systems
- ? Experience supporting security operation center (SOC) activities
- ? Experience working in an Agile environment both on premise and remotely
- ? Versed with ISSO 2700-Series. Authorized to work in the US for any employer

Work Experience Security Specialist

Akira Technologies Inc - Columbia, MD February 2019 to Present

Duties:

- Member of the Identity Management System Integrator (IDM SI) Scrum team providing support to enhance an effective delivery of IDM system integrator
- Function as a security specialist, a member of the security team performing various security activities to ensure the Identity Management (IDM) system obtains an authorization to operate (ATO) within client (CMS) stated date
- Supports the Security team in

developing, reviewing and updating ATO package artifacts of the IDM solution for completeness, correctness, and compliance Performs system categorization using FISP 199 and NIST 800-60 Volume 2 taking into consideration privacy concerns of the information IDM processes, transmits and stores Carry out security control selection for IDM system as well as coordinate with other system POCs to document security control implantation details Ensures security control implementation is in compliance with CMS Acceptable Risk Safeguards (ARS) and make sure all tasks performed by team members are in line with the statement of work (SOW) provided by the client. Collaborates with other IDM SI teams to develop the System Design Document (SDD), the Detail Design Review (DDR), and the Operation and Maintenance Manual (OMM) Plans tasks and collaborate with the different SMEs for inputs to develop ATO package documents to include System Security Plan (SSP), Risk Assessment (RA), E-authentication, Contingency Plan (CP), Contingency Plan Table Top Exercise, Contingency Plan Test (CPT), Incident Response Plan (IRP), Configuration Management Plan (CMP), and Change Management Plan as part of the ATO process

Attends meetings with team members, Client ISSO and other system stakeholders in effort to enhance the ATO process to meet deadlines Reviews ATO artifacts of FedRAMP systems interconnected with IDM. Submits daily planned tasks and report completed tasks daily and weekly to supervisors Planned, developed and maintains a schedule for IDM system controls implementation as well as maintain a tracking tool to monitor progress made Coordinate with CMS ISSO and other system stakeholders to ensure IDM system obtains an ATO within the stipulated deadline by the client Performs other security related functions as required by Akira and CMS Attend daily Scrum meeting to report on daily tasks completion and concerns IT Security Analyst

CWorld Security Ltd - Greenbelt, MD October 2015 to February 2019 Duties: Supported the Security Control Assessment Team to carry out assessment activities according to NIST standards Supported vulnerability assessments and penetration testing activities. Used DoD approved scanning tools to include but not limited to, NESSUS and Nmap Conducted FISMA-based security risk assessments for various government contracting organizations and application systems - including interviews, tests and inspections; produced assessment reports and recommendations;

conduct out-briefings. Documented and Review system security plans (SSP), contingency plans (CP), contingency plan tests (CPT), privacy impact assessments (PIA), and security assessment report (SAR) documents per NIST 800 guidelines for various government agencies Assisted in the development and maintenance of system security plans and contingency plans for all systems under my responsibility Maintained cooperative relationship with business partners or other interconnected systems Monitored controls post authorization to ensure continuous compliance with the security requirement Prepared and delivers documentation, reports and proposals to senior level personnel. Reviewed NIST standard on cyber security and incident handling (800-63, 800-61) Notified the responsible IT Security Officer (ITSO) of any suspected incidents in a timely manner, and assist in the investigation of incidents, as necessary Information Security Analyst CWorld Security Ltd - Greenbelt, MD October 2013 to September 2015 Duties: Performed categorization of information system using FIPS 199 as a guide or its equivalent NIST SP 800-60 Reviewed and updated some of the system categorization and security artifacts such as Initial Risk Assessment, E-authentication, PTA, PIA, SAR, SSP, SAP, MOU, ATO, ISA, DR, BIA & POA&M Assisted in the determination of an appropriate level of security commensurate with the impact level.

Assisted in the development of security plans, Contingency Plans, Disaster Recovery Plans, Incident Response Plans, and Configuration Management Plan Attended and supported A&A meetings with the government Contributing to initiate FISMA metrics such as Annual Testing, POA&M Management. Used Remedy ticketing system to create incidents and change management tickets Reviewed and provide updates on P-ATO and ATO cloud service authorization packages for interconnected FedRAMP Systems Fill-in and supported the Security Operations Center (SOC) team to monitor IPS (IronPort, FireEye, Sourcefire) for threats and vulnerabilities as well as used Jira, Remedy and ServiceNow to create incident tickets in accordance with client standard operation procedure (SOP) Used McAfee DLP to safeguard intellectual property and to ensure compliance by protecting sensitive data where it leaves Used McAfee Web Gateway proxy to grant web access request based on business justifications Cyber Caf Manager Fastline Internet October 2006 to June 2012 Duties: Performed general management for all three

cybercaf s owned by Fastline Internet Generated internet access tickets using server cybercaf pro

Provided troubleshooting for both clients and server PCs Formatted, configured, and provided networking for the cybercaf LAN Generated and emailed daily sales report to higher management

Performed daily back-up of the cybercaf pro database and restored when crash occurred

Enforced principles of least privilege and need to know to employee's user accounts Education

Masters of Science degree in Cyber Security Technology University of Maryland University College

(UMUC) 2017 to Present Associates Degree in Computer Science in Computer Science Prince

George's Community College - Largo, MD August 2017 Bachelor of Science degree in Information

Technology University of Buea October 2006 Skills Nist, Cyber Security, Information Security, Siem

Certifications/Licenses CCSK - Certificate of Cloud Security Knowledge August 2018 to Present The

CCSK certificate is widely recognized as the standard of expertise for cloud security and provides

the foundations needed to secure data in the cloud. Scrum Master Present A scrum master is the

facilitator for an agile development team. Scrum is a methodology that allows a team to

self-organize and make changes quickly, in accordance with agile principles. The scrum master

manages the process for how information is exchange ITIL v3 Certification August 2018 to Present

ITIL v3 is the third version of the Information Technology Infrastructure Library, a globally recognized

collection of best practices for managing information technology (IT). AWS - Amazon Web Service

Certified Developer Present CompTIA Security+ CE August 2018 to August 2020 CompTIA

Security+ is a global certification that validates the baseline skills you need to perform core security

functions and pursue an IT security career. Slunk 7.x Fundamentals August 2018 to Present Splunk

provides the industry-leading software to consolidate and index any log and machine data, including

structured, unstructured and complex multi-line application logs. Additional Information TECHNICAL

SKILLS: Microsoft Suite (Word, Excel, PowerPoint, Outlook) Linux Microsoft windows OS

VMWare Nessus Nexpose Nmap Splunk WebInspect Snort Wireshark Assessment &

Authorization(A&A) OSI Model IronPort FireEye Sourcefire McAfee Web Gateway McAfee DLP

Confluence SharePoint Jira Remedy ServiceNow CFACTS GRC Risk Vision

Name: Jeffrey Mcdonald

Email: smithbrenda@example.com

Phone: 397-419-9630