IT Security Analyst IT Security Analyst IT Security Analyst - Jelani Consulting Lanham, MD An organized result oriented Cyber Security Analyst with over 2 years of experience in analyzing security incidents with the zeal to learn new technologies in a short time and work with them. Specialized in proactive network monitoring of SIEM (Security Information and Event Management) tool such as Splunk. Performs malware analysis with the overall objective to ensure confidentiality, integrity and availability of the systems, networks and data. Working knowledge of Risk Management Framework (RMF) Processes and Workflow. Skilled in assembling security authorization package using NIST SP 800-60 Vol 2, FIPS 199, NIST SP 53 Rev 4, FIPS 200, NIST SP 800-18, NIST 53A, NIST SP 37. Proficient in the preparation and updating of System Security Plan (SSP), Security Assessment Plan (SAP) Work Experience IT Security Analyst Jelani Consulting July 2017 to Present Responsibilities: Communicate security and compliance issues in an effective and appropriate manner, and recommend remedial actions to mitigate risks, and ensure information system employ appropriate level of information security controls Use Splunk (SIEM) to monitor and correlate security events and alerts Monitor incoming incident tickets from the CSC, triage, and prioritize events and alerts. Develop SOPs for tasks such as IOC investigations and blocks, addressing suspicious emails, host and user identification, and more. Upload IOCs from third-party intelligence reports to monitoring tools(Splunk). Develop procedures and handle user-reported cases of potential security incidents in accordance with SOC processes and procedures. Create and compile daily situational awareness reports. Identified false/real threats, analyze tool alerts, identify Host involvement, compare scan results, identify incident/events, determine priority level(s), analyze logs, validate IP addresses, identify customer POC, Incident creation, open a Triage Line, document incidents, communicate incidents, and gather incident details. Analyzed and investigated security events utilizing open source tools (VirusTotal, Blue-Coat's sitereview, MX Tool Box, Domain Tools, Talos Intelligence, JoesSandbox, Hybrid analysis, Central Ops, etc. Collaborating with Security Operations Center Engineers, NOC, the SOC tier 2, 3, 4 Analyst, CSIRT team to rapidly monitor and analyze detection rules as needed to help enhance the security of the organization as well as tune existing security tools, and services.

Ensuring the integrity and protection of networks, systems, and applications using the organizations security policies, through monitoring possible threats, vulnerabilities, and the organizations infrastructure. Examine firewall, database, and other log sources to identify malicious activity Research the latest Information Technology trends and recommended security enhancement to the management team Support review of policy, security alerts, regulations and technical advances in IT security management Monitor the Remedy queue, manage and respond to trouble tickets Monitor Network Traffics, alert, intrusion attempts and documented report of security breach to the management team Assist in tracking unresolved weakness to ensure they were mitigated based on the organization securities baselines Perform vulnerabilities scanning using Nessus to ensure securities controls were operating effectively and to detect flaws Participated in daily and weekly security operations with SOC lead, ISSO, ISO, project managers, to report and and outline proposed solutions to meet the delivery needs. Perform accurate and precise real-time analysis and correlation of logs (Email logs from IronPort, Intrussion logs from SEP) and alerts from different devices to determine whether the events constitute security risk/incidents. Analize and investigate potential, successful, and unsuccessful intrusion attempts and compromises thorough reviews and analyses of relevant event detail and summary information. Worked in a 24x7 Security Operations Center Monitoring and analyze security events to determine intrusion and malicious events. Search firewall, email, web or DNS logs to identify and mitigate intrusion attempts. Investigate malicious phishing emails, domains and IPs using Open Source tools and recommend proper blocking based on analysis. Security Operations Analyst Solutions Inc June 2016 to June 2017 Responsibilities: Participated in daily and weekly project planning sessions with project managers, business analysts and development team to analyze business requirements and outline proposed solutions to meet the delivery needs. Develop, review and update Information Security System Policies, System Security Plans (SSP), and Security control baselines in accordance with NIST, FISMA, OMB App. III A-130, NIST SP 800-18 and industry best security practices. Develop policy and procedural controls relating to Management, Operational and Technical Controls for the Organization. Perform the role of Security Control Assessor of General Support Systems (GSS),

major Applications and Systems to ensure that such environments are operating within the strong security posture. Create ATO package documents; SSP, SAR and POAM based on the security assessments performed on systems. Apply appropriate information security control for Information System based on NIST 800-37 rev1, SP 800-53 rev4, FIPS 199, FIPS 200 and OMB A-130 Appendix III. Review and update some of the system categorization using FIPS 199. Develop Contingency plans, Disaster Recovery Plans and Incident Response plan for Information Systems using NIST SP 800 - 34. Perform continuous monitoring after authorization (ATO) to ensure continuous compliance with the security requirements Ensure timely completion and testing of all POA&M actions to meet agency deadlines Communicate effectively through written and verbal means to co-workers and senior leadership Perform Security Assessments to determine if controls were implemented correctly, operating as normal and meeting desired objectives. Recommendations, and identification of security controls for systems, and networks. Perform the role of Security Control Assessor by reviewing the artifacts and implementations statements provided by the ISSO on a system to determine if the security controls are yielding the desired result. Develop systems that assist the organization to secure the CIA by categorizing and selection of controls using NIST SP 800 60, 800 53 and FIPPS 199 and 200. Technical skills: Microsoft Office Suite, Windows, Mac, Knowledge of Network Security Devices & Configurations, Splunk, Symantec, BMC Remedy, FireEye, Cisco IronPort, Cofense Triage, Tenable SecurityCenter-Nesus, ServiceNow, VPN, OSI/TCP/IP, Firewalls, and IDS/IPS Systems, Knowledge of Regular Expressions. Education Masters of Business Administration in Business Administration University of Chester UK - Chester 2014 Skills Ids, Ips, Splunk, Vpn, Cisco, Firewalls, Network security, Remedy, Tcp/ip, Security, Tcp, Bmc, Symantec, Microsoft office, Mac

Name: Lisa Carey

Email: brittanylewis@example.com

Phone: 722-517-2140