SOC Analyst SOC Analyst SOC Analyst - Prosec Solutions Hyattsville, MD Monitoring network traffic for security events and perform triage analysis to identify security incidents. Identifying potential threat, anomalies, and infections. Responding to computer security incidents by collecting, analyzing, providing details evidence (network log files) and ensure that incidents are recorded and tracked in accordance with its guideline and requirements. Documenting findings from analysis. Providing recommendations within the incident-management system. Review and analyze pcaps using Wireshark. Conduct vulnerability scanning using Nessus Monitor client SIEM devices (Splunk) for potential security events that could compromise the client's environment.

Perform email analysis to determine if the email is malicious, spam, phishing, or scam Recommend next steps to users on how to proceed with the suspicious emails Conduct Malware analysis and investigate behavioral characteristics of each incident utilizing IDS monitoring tools. Conducted research on emerging security threats. Ensure the integrity and protection of networks, systems, and applications by technical enforcement of organizational security policies, through monitoring of vulnerability scanning devices. Authorized to work in the US for any employer Work Experience SOC Analyst Prosec Solutions March 2016 to Present Monitoring network traffic for security events and perform triage analysis to identify security incidents. Identifying potential threat, anomalies, and infections. Responding to computer security incidents by collecting, analyzing, providing details evidence (network log files) and ensure that incidents are recorded and tracked in accordance with its guideline and requirements. Documenting findings from analysis. Providing recommendations within the incident-management system. Review and analyze pcaps using Wireshark. Conduct vulnerability scanning using Nessus Monitor client SIEM devices (Splunk) for potential security events that could compromise the client's environment. Perform email analysis to determine if the email is malicious, spam, phishing, or scam Recommend next steps to users on how to proceed with the suspicious emails Conduct Malware analysis and investigate behavioral characteristics of each incident utilizing IDS monitoring tools. Conducted research on emerging security threats. Ensure the integrity and protection of networks, systems, and applications by technical enforcement of organizational security policies, through monitoring of

vulnerability scanning devices. IT Security Analyst Charles Ego C.P.A July 2014 to March 2016 Categorized systems based on SP -800-60 in order to select the appropriate NIST recommended control SP 800-53. Developed, reviewed and updated Information Security System Policies and System Security Plans (SSP) in accordance with NIST, FISMA and industry best security practices. Updated IT security policies, procedures, standards, and guidelines according to department and federal requirements. Coordinated and performed reviews of data center general controls, operating systems, systems development life cycles and monitored procedures relating to physical security over data centers and computer operations. Conducted IT controls risk assessments that included reviewing organizational policies, standards and procedures and provided advice on their adequacy and accuracy. Updated contingency plan and conducted contingency plan test. IT Auditor Charles Ego C.P.A July 2012 to June 2014 Tested IT general and application controls, and performed walkthroughs and detailed testing of controls to evaluate the design and operating effectiveness of controls in commercial entities. Assessed internal controls using COBIT framework in various sectors such as financial, retail, energy and technology. Performed audit of IT general and application controls, information security, systems development, change management, business continuity, disaster recovery and computer operations. Performed IT general controls testing for Sarbanes-Oxley 404 compliance in public companies, OMB A-123 in government agencies, and Service Organization Control (SOC) reports in compliance/SSAE16 (formerly SAS 70). Participated in SAP Transaction testing to perform, including testing of segregation of duties to assist the client in improving their user management, authentication management, authorization management, access management, and provisioning capabilities. Tested General Computer Controls and Business Process Application controls using FISCAM and FISMA frame work and performed walkthroughs and detailed testing of controls to evaluate the design and operating effectiveness of controls in federal government agencies. Education Certificate in Cyber Security Frederick Community College May 2017 M.B.A. in Certified Information Systems Auditor University of Maryland University College May 2014 M.S. in Financial Management & Information System University of Maryland University College May 2013 Skills NESSUS (3 years),

SPLUNK (3 years), WIRESHARK (3 years), FEDERAL INFORMATION SECURITY MANAGEMENT ACT (2 years), FISMA (2 years) Additional Information TECHNICAL SKILLS Splunk, Wireshark, FireEye, Nessus, SAP, Linux, Windows, NetSuite, SOX testing, VMware, COBIT, COSO, FISCAM, A-123, SSAE 16/SAS 70, NIST-SP-800 Publication, FISMA framework, Microsoft Word, Access, Excel, PowerPoint, Outlook, Microsoft Project, Microsoft Visio.

Name: Mary Hernandez

Email: virginia55@example.com

Phone: +1-857-206-6009