Cyber Security Analyst Cyber Security Analyst Cyber Security Analyst - Flex Enterprise Ridgeland, MS Bachelor's degree in Computer Science & Engineering. More than Five years of information security experience. More than Three years of hands-on security operations experience including interdisciplinary experience with Cyber Threat Analysis, Digital Computer Forensics, Incident Response, Application Security, Operating Systems Security, Cryptographic Controls, Networking. Technical experience and comprehensive knowledge of threat actor capabilities, intentions, methodologies and motives. Familiar with computer network exploitation and network attack methodologies. Willing to relocate: Anywhere. Authorized to work in the US for any employer. Work Experience Cyber Security Analyst Flex Enterprise - Ridgeland, MS February 2016 to Present Core Responsibilities: Administers security controls to prevent hackers from infiltrating company information or jeopardizing e-Commerce programs. Maintains security systems for routers and switches. Administers security policies to control access to systems. Maintains the company's firewall. Uses applicable encryption methods. Provides information to management regarding the negative impact on the business caused by theft, destruction, alteration, or denial of access to information. Assessment and Authorization (A&A), Certification and Accreditation (C&A) IT Security Compliance. HIPPA, PCI-DSS 3.2, ISO 27002, NIST Vulnerability Assessment and Scanning, Penetration Testing Network Security, Intrusion Detection and Prevention, Data Loss Protection. Information gathering and Assurance Risk Assessment and Management Systems Development Life. Cycle Design, Architecture, implementation and Roll out of Perimeter Security related Controls like ATP, Firewalls Compliance and Audit Security Incident and Event Monitoring (SIEM). Virus Infestations and Network Abuse Investigations Malware Analysis. Cyber Threat Intelligence. Cyber Incident Response. Receiving, documenting, and reporting cyber security events. Categorizing incidents and implementing corresponding escalation procedures. Communicating and coordinating incident response efforts. Conducting operational update meetings for SOC staff. Analyzing reports to understand threat campaign(s) techniques, lateral movements and extract indicators of compromise (IOCs). IT Security Control Assessor / SOC Analyst IIT Consulting - Beltsville, MD February 2015 to January 2016 Cyber Security Operations Center (SOC) Analyst: Performed daily

operational monitoring of events and alerts from multiple sources, including our Security Information and Event Management (SIEM) and IDS/IPS tools, malware prevention platform, system logs. Investigated events to either remediate or escalate further. Responsible for providing accurate & priority driven analysis to detect, analyze, respond to and track security threats and vulnerabilities. Utilized information security tools to gather information needed to investigate events of interest. Coordinated with business units, operations, and technology teams for incident response, remediation, and improvement. Created and maintained documentation, processes, procedures, and reports. Contributed to the continuous improvement and growth of the SOC and Information Security unit. Security Controls Assessor: Supported client Security policies and activities for networks, systems and applications including Vulnerability Management, Incident Reporting, Mitigation, and Continuous Monitoring Prepared Security Assessment and Authorization (SA&A) packages for information systems in compliance with Federal Information Security Management Act (FISMA) utilizing National Institute of Standards and Technology (NIST) Special Publications (SP) 800 series. Worked closely with the Office of Chief Information Security Officer to keep the systems complaint with information system continuous monitoring reporting requirements. Monitored VPNs, server logs, firewall logs, intrusion detection/prevention logs, network traffic and other security systems for unusual or suspicious activity and reported such activity to appropriate individuals within the team. Work with both internal and external resources to conduct security audits, addressed gaps, and ensured compliance with regulatory and industry requirements. Information Assurance Analyst Lenox Medical Group - Washington, DC April 2010 to February 2015 Prepared and updated system security plans on a regular basis to provide an accurate up to date overview of the information systems. Prepared information system categorization for information systems using Federal Information Processing Standard Publication and NIST SP Conducted security control assessment; prepare security assessment plans, reports, and plan of action and milestones Prepared privacy threshold analysis and privacy impact assessment utilizing e-Government act of 2002 Prepared business impact assessment and contingency plans; provided contingency plan training and testing. Developed procedures and methodologies for Security Authorization activities.

Reviewed application change requests to assess security impacts to the application and organization. Conducted compliance reviews of the security authorization packages prepared by other organizations and provide a report to the office of the Chief Information Officer (CIO). Reviewed security logs to ensure compliance with policies and procedures and identifies potential anomalies. Managed vulnerabilities with the aid of Nessus vulnerability Scanners to detect potential risks on a single or multiple assets across the enterprise network Reviewed SAR post assessment. Created and completed POAM's milestones to remediate findings and vulnerabilities. Updated, reviewed, and aligned SSP to the requirements in NIST 800-53, rev4. Monitored security controls post authorization to ensure continuous compliance with the security requirements. Communicated analysis, design, and specifications both functional and technical to all supporting organizations. Collaborated and directed efforts within Quality Assurance to ensure desired results. Supported Security policies and activities for networks, systems and applications including Vulnerability Management, Incident Reporting, Mitigation, and Continuous Monitoring. Security Compliance Analyst St. Augustine Group - Laurel, MD February 2009 to February 2010 Security Compliance Analyst: Responded to medium and high severity incidents (coordinating with numerous groups involved in responding to incidents, as well as conducting follow-up investigations to such incidents.) Proactively managed incidents to minimize customer impact and meet SLA's. Identified trends to optimize incident processes and monitoring tools. Worked closely with the Security Operation Center, Legal and Loss Prevention teams to support tier 1 and 2 security incident management. Investigated network intrusions and other cyber security incidents to determine the cause and extent of compromise. Performed host-based and network-based analysis across all major operating systems and network device platforms. Assisted in development and implementation of courses of action (COAs) that focus on containment, eradication, and recovery. Ensured the acquisition and preservation of data required for tactical analysis, strategic analysis, and/or LE investigations. Collaborated across all IT departments - (Security Engineering, Network Operations, Access Management, Legal). Recommended effective process changes to enhance defense and response procedures. Produced security incident and investigation reports/briefings. Provided consultation,

guidance, and assistance to other departments on the design, implementation, and operation of appropriate technical, physical, and administrative controls to ensure the security of the company's sensitive information Education Bachelor of Science in Computer Science & Engineering Enugu State University of Science & Technology Skills SECURITY (8 years), TESTING (6 years), NESSUS (4 years), SIEM (2 years), FIREWALLS (1 year) Additional Information SKILLS Firewalls (PaloAlto Networks, Checkpoint, Cisco ASA, Juniper) Log Management and SIEM (Splunk or HP ArcSight, QRadar) Network Analysis Tools (Wireshark) System Analysis and Forensic Tools (FTK, EnCase) Endpoint Security (Symantec, McAfee, Forefront) Windows Management (WSUS, SCCM, SCOM, Active Directory, Group Policy Objects,) Vulnerability Management (Nexpose, Tenable Nessus, Qualys) Penetration Testing Tools (Metasploit, Backtrack, Kali) Operating Systems (Windows Server 2008/2012, CentOS Linux, OSX) Enterprise Microsoft Solutions (Exchange, Sharepoint, Lync) Regulatory Regimes (ISO27K, HIPPA, PCI, FISM)

Name: Thomas Hicks

Email: wfrey@example.com

Phone: 627-962-0073x887