IT Risk Analyst IT Risk Analyst IT Risk Analyst - NYC DEPARTMENT OF INFORMATION TECHNOLOGY - CYBERCOMMAND Saddle Brook, NJ To secure a position within a reputable organization with the aim of leveraging my knowledge & skills in enhancing organization security posture. Possess experience in GRC, risk management framework (RMF), information & information systems management, vulnerability management, and system development life cycle (SDLC). Authorized to work in the US for any employer Work Experience IT Risk Analyst NYC DEPARTMENT OF INFORMATION TECHNOLOGY - CYBERCOMMAND - New York, NY March 2018 to Present Develops and update Risk Management plan. Assess and audit agencies' security controls and make recommendations based on findings and security framework used. Works with multiple government agencies. Implements GRC processes and plans - assess enterprise-wide risks, writing and updating security policies and procedures followed by governmental agencies, and enforcing executives order. Assess agencies' assets for potential and active vulnerabilities and/or risks. Implements remediation processes to mitigate possible threats on third party vendors' assets. Conducts host discovery scan (enumeration), port scan, vulnerability scan, and web-application scan using scanning tools. Configures web-application and vulnerability scan for authenticated and/or un-authenticated scan. Analyze web application and vulnerability scan results paying more attention to the severity level of vulnerabilities such as top priority, malware exploitable, popular target, zero day, predicted exploit, easily exploitable, and active net breaches etc. Ensuring that vulnerabilities are remediated on time based on its level of severity. Uses ticketing tools to manage and track remediation of web application vulnerabilities and network vulnerabilities. Implement web applications patch updates as required and/or based on scanning tool recommendations. Analyze vulnerability scan results of agencies and provide high level remediation steps to implement. Review vulnerability management and security automation tools for efficiency while in POC or before deployment into production. Familiar with many vulnerability and threat management security tools. Reviews the SDLC of applications ensuring compliance is followed by App developers. This involves Software Security Assurance process. Categorizes data in applications, and critical IT infrastructures. Ensures that in-house

grown, modified COTs, and COTs applications meets the appropriate security requirements before approval for deployment and/or production. Assess security controls and make recommendations as needed. Writes security policies and update security policies as needed. Manage and monitor access to security scanning tools such as Tenable.io and Rapid7. Ensures that NIST security framework is followed and implemented. Use Google Doc, Google Sheet, Google Slides, Google Forms, Google Drive, Excel spreadsheet, OneNote, and Sharepoint for required workflow. IT Security Analyst CYBERSOFT TECHNOLOGIES INC - Lanham, MD November 2016 to February 2018 Monitored existing security controls against the risks of potential vulnerabilities being exploited by threats. Conducted risk assessment on third party vendors' assets and/or information systems. Make recommendations and/or implement appropriate security controls on third party vendors' assets to ensure optimal security posture. Responsible for effective backup & recovery strategy to ensure availability of data in case of major security attacks or natural disaster. Use Excel to manage work-flow such as Risk score calculation using metrics. Used NIST SP 800-60 & FIPS 199 to determine system categorization of organizations' assets by evaluating information types and then relate them to the security objectives (Confidentiality, Integrity, & Availability) Responsible for determining the classification of information systems, impact levels, assess existing security controls and recommend alternative controls to include technical, management & operational to enhance the security posture of organization if necessary When working on projects, responsible for developing a security authorization package, consisting of; (i) System Security Plan (SSP), (ii) System Assessment Report (SAR), and (iii) Plan of Action & Milestones (POAM) Conversant with risk assessment plan, business impact assessment, continuous monitoring strategy, data loss prevention, disaster recovery plan / contingency plan, configuration management plan, information & information security management, security assessment plan, system architecture diagrams, & incidence response plan. Performed vulnerability scanning using Nessus & Rapid7, Tenable.io, Qualys, OpenVAS, Nmap etc. Information System Security Analyst NETWORK DYNAMICS INC - Owings Mills, MD December 2014 to October 2016 Performed vulnerability scanning using Nessus & Retina ensuring low or no false positives. Planned as well

as conducts assessment of data processing systems applications to safeguard assets, ensure accuracy of data, and also promote operational efficiency. Responsible for reviewing all new technologies, services, solutions and processes and offering advice to ensure security and alignment with best practices. Risk analysis of threats identified by the vulnerability scanning, reporting to the client on severity, exposure, likelihood of compromise and potential consequences.

Developed, maintained and enforced Information Security standards, polices and guidelines relating to IT Security by addressing ISO27002 guidelines. Evaluated, certified and inspected all technical and non-technical system controls for compliance. Performed security administration, monitoring for designated systems and resources. Performed risk assessments by identifying points of vulnerability, made recommendations for disaster avoidance and reduction strategies which reduced unnecessary costs. Recommended mitigating actions to increase protection of key information assets, improve security incident response by increasing the value proposition of managed security services. IT Support/ Analyst BRONX LEBANON HEALTH SYSTEM - Bronx, NY June 2010 to November 2014 Provided training & support to providers (MD, PA, NP) on the use of electronic health information system. Implemented strong security controls and password complexity and ensured staff complied to them Developed an effective plan to improve medical practices via electronic system. Troubleshoot systems errors, malfunction or glitches Ensured that electronic health records (EHRs) and CPOE are running smoothly Installed and configured software and related products Established effective Backup & Recovery policies & procedures, also created and maintained users and roles Assigned and revoked user privileges using least privilege and role-based policies (maintained database security) Worked in conjunction with developers to design and implement databases Education ISC Master of Science degree in Information Technology CyberSoft Technology Institute - Lanham, MD Bachelor's Degree Grand Canyon University - Phoenix, AZ University of Texas - Arlington, TX Skills Excel (2 years), Nessus (3 years), scanning (4 years), security (8 years), System security (3 years) Additional Information SKILLS & EXPERTISE: Experience in vulnerability management and remediation process. Ability to run vulnerability scan, using Tenable.io, Nessus, Rapid7, Qualys, Nmap, and OpenVAS

scanning tools. Experience in host discovery (enumeration), port scanning, advanced scan, and authentication scan. Conversant using Excel - able to use VLOOKUP and HLOOKUP functions. Auto-save email attachments to csv format in Excel. Creating and managing Excel tables, creating metrics, and diagrams such as Heat maps, histograms, pie-charts and many more. GRC (Governance, Risk Management, and Compliance) experience in governmental sector. Framework familiar with are NIST, CIS-CSC, CoBIT, HIPAA, CoSo, ISO. Experience in risk control and assessing third party critical assets for any potential vulnerabilities and threats. Familiar with FIPS 199, FIPS 200 & NIST Special Publications 800-30 & 37, 800-39, 800-53A & Rev4, 800-60, 800-70, 800-115, 800-137, and CSF framework etc. Understand the importance of backup & recovery, and system disaster recovery plan. Experience in evaluating, analyzing, and managing risk using Risk Management Framework (RMF). Ability to develop and analyze a System Security Plan (SSP), Security Assessment Plan (SAP), Security Assessment Report (SAR), and also a Plan of Action & Milestones (POAM). Extensive experience in implementing a robust continuous monitoring strategy to ensure a secured environment. TECHNICAL SKILLS: Kali-Linux, knowledgeable in Pen-testing, Git tools (GitHub), Linux (Command Line), Vulnerability scan, Scan configuration, Project management tools - Clarity, Jira, Trello. Ticketing tool - BMC-Remedy and Jira, Operating Systems: Windows. Microsoft Office Applications, Access Control, Identification & Authentication.

Name: Michael Watkins

Email: timothymorales@example.net

Phone: +1-418-726-1639x18304