IT Project Lead IT Project Lead IT Project Lead - Altria/Phillip Morris USA Richmond, VA Work Experience IT Project Lead Altria/Phillip Morris USA - Richmond, VA November 2018 to Present * Provide analysis, deliverables and mitigation of all technical activities related to Cybersecurity. * Maintain focus and provide clear direction to both team members and with respect to external influencers * Provide an honest assessment of the project relative to current and future cost * Understand the scientific rationale and technical issues associated with the project target and lead agents * Making sure all team members and their line managers and key stakeholders support the project * Keep team members and stakeholders informed of key developments, program decisions, issues, and changes to the project and the project plan Penetration Tester 1st IO Command - Fort Belvoir, VA July 2012 to September 2018 * Enhance security for US army networks as a Penetration Tester for the First IO CMD detachment * Charged with discovering and exploiting vulnerabilities to increase network integrity * Utilize creativity, imagination and extensive technical knowledge to effectively troubleshoot and resolve security issues * Design and implement penetration and security testing procedures, and maintain full compliance with security regulations to protect sensitive data * Implement patching policies to ensure system security; design and administer security patching policy for all network servers * Develop technical writing documents of after-action reports based on findings from a security posture assessment. * Participate in the planning stages to of the cyber assessment plans. Observe command exercises to later be assessed and modified based on feedback. SIEM Engineer Horizon Industries - Richmond, VA April 2017 to April 2018 * Perform routine security audits bringing department assets into compliance * Utilize creativity and extensive technical knowledge to effectively troubleshoot and resolve security issues * Develop, implement, and maintain security technologies that improve the security of the organization's network and services * Provide technical solutions for incidents, architecture and reporting * Implement patching policies to ensure system security; design and administer security patching policy for all network servers Cyber Security Consultant Veris Group, LLC - Vienna, VA March 2016 to April 2017 * Work with Federal clients to mitigate cyber risk and threats * Identify opportunities for efficiencies in work process and innovative approaches to completing scope of work * Actively

expand consulting skills and professional development through training courses, mentoring, and daily interaction with clients * Participate and contribute to various project and status meetings; report project status to the Project Manager, problem resolution and collaboration on project planning and execution. * Develop and execute security policies, plans, and procedures. * Prepare, review, and/or update, and maintain IT Security supporting artifacts SIEM Analyst Insight Global - Fort Belvoir, VA July 2015 to March 2016 * Provide level 3 SIEM support to manage SIEM components, IDS/IPS, parsing/normalization of logs, rule engine, log storage, source device, log collection and event monitoring * Solid working knowledge of networking technology and the OSI Model, including TCP/IP protocols and standards. * Review security logs and violation reports for root cause analysis * Expertise with tools and processes used in security incident detection and handling * Monitor and recommend improvements based on events or incidents of apparent security breaches in areas including networks, applications, databases, systems, and endpoints * Develop filters and correlated event rules to reduce false-positive alerts. Cyber Security Technician Hewlett Packard - Arlington, VA April 2014 to July 2015 * Implement information security programs and schedule system updates to increase system security * Investigate and protect the network against Web threats including malware, phishing, viruses, denial-of-service attacks, information warfare and hacking * Analyze, troubleshoot, and investigate security-related anomalies based on security platform reporting, network traffic, log files, host-based and automated security alerts * Monitor and analyze corporate network traffic for security breaches, breach attempts, reconnaissance, denial of services attacks and other security events * Proactively protect applications and servers from attacks by deploying countermeasures and tools to better secure the organization's infrastructure * Provide and maintain the overall operational quality, service delivery and aid in maintaining the required compliance of security systems Education Bachelor of Science in Business Management University of Virginias College at Wise - Wise, VA 2011 Skills INFORMATION SECURITY, METASPLOIT, NESSUS, NMAP, SNORT Links http://www.linkedin.com/in/marcwilliams31 Additional Information Core Competencies * Data-at-Rest SME * Proficient w/ Bash Scripting * Team Based Troubleshooting * Encryption

Tech Lead * Security Awareness * Project Liaison * Event Log Collection * Security Governance * Hyperfocus * Cyber Threat Incident Management * Vulnerability Management * Data Leakage Prevention Selected Skills & Highlights * Experienced Penetration Tester for the US Army Reserves and in the private sector * Master troubleshooter, proficient in evaluating system security and developing technical solutions quickly * Excellent communication skills proven by the ability to lead and interact with people from diverse backgrounds * Researches the latest information technology (IT) security trends * Conducted Cybersecurity pre-execution site surveys and Cybersecurity architecture review * Executed cybersecurity test requirements and improved process and practices * Developed cybersecurity test designs to support Operational Test Directors * Developed representative exploitations to fully test the cybersecurity of any system under test * Manually examine system and network configurations, system logs, and devices * Implements Information Security Vulnerability Management, Alerts, Technical Advisories and Bulletins in accordance with Component/Organization policies * Provides technical support and recommendations in maintaining the integrity, accessibility, and confidentiality of the information systems Technical Skills Operating Systems: * Windows Server 2003-2012, Windows 7-10, RHEL 7, Linux/Unix, iOS, MacOS, Android Security: * Microsoft Security Baseline Analyzer, Nessus, Snort network intrusion detection and prevention system, Symantec Endpoint Protection, Arcsight, Zenoss, Nagios, Wireshark, Qradar, User Behavioral Analysis Pentesting: * Cobalt Strike, Empire, Burp Suite, Metasploit, Nmap, Nikto, Hashcat, MSFConsole, TCPDump

Name: Stephen Beltran

Email: michael99@example.net

Phone: 930.943.9059x2504