Sr Security Analyst Sr Security Analyst Sr Security Analyst - Home Credit Blue Springs, MO Over 17 years' experience professional in IT (Information Systems, Security, Compliance). Expert in Vulnerability Management with a solid understanding of security architecture, policies and security capabilities of major operating systems & platforms. Holder of 2 patents (Design & utility). Founder of a nonprofit organization called Safety52 that focuses on providing smart technologies to enhance the lives of children and the elderly. Authorized to work in the US for any employer Work Experience Sr Security Analyst Home Credit January 2016 to Present   Manage and administrator QRADAR, MDM Mobile Iron & Mass360 Qualys, CyberArk.    Manage events and incident reporting and documentation in Omnitracker for IT Security. Send Monthly reports.    Manage KnowBe4 users, training and campaigns for Security Awareness and implement training videos for employees. Install MDM Mobile Iron for BYOD and company phones. Manage Vulnerability scans in Qualys and coordinate remediation efforts.    Monitor Qradar offenses and assign and close out offenses. Gather evidence from Security assessments. Review and update Security Policies.    Assist with identifying and anticipate risks and issues and with mitigation.    Manage and maintain policy, procedure and associated governance documentation related to organization aligned security compliance methodologies.    Provide Assistance with incident response documentation, risk assessment and third party audit documentation and remediation tracking.    Define the security direction for the organization, including systems, networks, user services, and vendor development efforts.   Develop relationships and engage with industry partners, Security Information Exchanges, and other groups to assess industry advances in technical security technologies.    Assess security industry trends and provide consultation, recommendations, and implementation advice on emerging technologies.    Test potential security solutions to validate features and functions, partnering with other organizations in the resolution of interoperability issues to obtain successful integration of security solutions across all platforms.   Consult with senior management and internal clients across multiple business units on complex security topics and policy interpretation. Proactively identify potential security issues within the corporate and carrier infrastructure and provide strategic direction to avoid risks to assets.   Ensure reports and findings are delivered in a

timely and appropriate manner to management, operations, and executive leadership and understand new laws and regulations and provide consultation, recommendations, and implementation advice to the organization. Make necessary adjustments to the Information Security Policy. Vulnerability Management Analyst BCD Travel January 2015 to January 2016 Coordinated and delegated vulnerability remediation efforts. Performed vulnerability scans on the Rapid 7, Nexpose scanner for internal scans. For PCI scans, performed scans using solutionary for the external scans. Remediated over 19,000 vulnerabilities by decommissioning assets and by performing normal Nexpose cleanup. Prioritized workflow of staff to ensure efficient use of resources and completion of work. Created standards and policies, and reviews written reports, papers, and correspondence for accuracy, consistency, style and clarity. Consultant KCPL August 2014 to January 2015 Scheduled and launched periodic audit reviews for change management. Planned and oversaw risk mitigation and remediation projects using Qualys. Developed and delivered risk awareness training for key staff and stakeholders. General understanding of North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) standards. Security Analyst Ericsson June 2014 to August 2014 Planned and oversaw risk mitigation and remediation projects utilizing Nessus and Rapid 7. Managed over 20,000 assets for vulnerability remediation. Worked with appropriate Technical system owners and application owners for vulnerability remediation. Managed 2 staff and delegated responsibilities toward remediation efforts. Effectively delegated assignments to provide reasonable challenge and developmental opportunities for supervisors and staff to strengthen depth and breadth of knowledge. Compliance Analyst Swiss RE November 2013 to May 2014 Managed a staff of 5 in London, India. Delegated and coordinated audits. Promoted awareness of security issues among management and ensure sound security principles. Translate applicable industry regulations and integrate into policy. Defined and/or implemented policies and procedures to ensure protection of critical infrastructure. Increased awareness of the information security policies within the corporation by designing, developing and presenting training. Consulted and collaborated with organization's IT leaders, security officers, human resources department, and legal counsel to ensure full legal compliance of

company policies, procedures, forms, notices, and materials.   Worked closely with IT department to develop and coordinate a compliance schedule tailored to the applicable regulations.    Worked closely with IT departments on corporate technology development to fully secure information and information-processing/gathering systems.   Oversaw automation of internal controls and centralize logging and reporting.      Managed securing of all platforms and centralize security event management.   Acted as liaise between internal and external audit teams.   Managed the SOX and PCI audit processes for the IT department, including resulting action items, process changes and improvements.     Scheduled and launched periodic audit reviews.     Planned and oversaw risk mitigation and remediation projects using Qualys.     Developed and delivered risk awareness training for key staff and stakeholders. Sr. Security Analyst/ IT Consultant Cerner Health May 2007 to August 2010   Created Security Policy, departmental procedures and Service Level Agreements, (SLA's. Performed File Level Permission reviews and managed the retention of related audit documentation.     Configured automated reports and notifications to proactively monitor security of the critical components.   Provided malware and virus remediation.    Established security strategy of protecting Process Control Networks.     Utilized SEIM such as Tripwire and NMAP tools and Cerner Core Security.     Ran vulnerability scans using Qualys and informed appropriate business owners about vulnerabilities needing remediation. IT Security Compliance Consultant Agilysys, Inc August 2006 to May 2007     Conducted and analyzed weekly vulnerability assessments and coordinated remediation efforts using Rapid 7.     Met with executive staff to help guide security postures in a direction that protects the company while not impacting business growth or function. Worked with executive staff and business unit leaders to educate them on current APT (Advance persistent threat) Malware and other security threats.    Worked with the executive team to develop employee security awareness training programs .Conducted training to employees and staff. Worked with the Executive, Shared Services and Business leadership to align the IT organization with business unit security and compliance needs.     Developed and institute security and compliance goals and objectives.    Developed and communicated security strategies and plans to executive team, staff, partners, customers, and stakeholders.     Established guiding principles

compliance management. Reviewed proposed projects to identify potential risks. Projected and tracked costs of risk management initiatives. Identified and deployed standard risk assessment models or frameworks. Selected and deployed appropriate best practices using governance frameworks, such as COBIT. IT Systems Analyst Hartford Life Insurance Group CT 2006 to 2006 2006 Provided quality control analysis, summary results, and details as well as recommendations for improvement. Functions of the area include the following: auditing, reporting, notifying management of error trends and/or recommendations for improvement, procedure change recommendation mitigating controls and documentation and procedure maintenance. Provided measures and metrics summarizing the quality levels and error trends. Review, analyze, and test key (Sarbanes-Oxley/"SOX404") control processes. Assisted in Recertification for applications such as PeopleSoft, Business Objects, Pyramid, Solar, Track, review, and analyze operational effectiveness testing remediation items for RBAC. Systems Analyst UPS Corporation - Mahwah, NJ January 2001 to July 2005 Worked with support organizations to identify Infrastructure enhancement. Coordinated with global cross discipline engineering teams. Evaluated and integrated vendor systems solutions, interoperability products, operating systems and patches and internal and external solutions. Architected solutions for storage, high availability, clustering, disaster recovery, operating systems migration, software distribution and inventory management. Integrated, tested, and certified all architectural standards. Provided event notification management for open systems and Mainframe. Documented business processes for the business analyst team. Developed and presented alternative solutions to solve business needs. Developed process, use case, and other associated requirements documentation (business rules, data specification, prototypes etc.) to accurately describe business requirements. Administered and Implemented a SAN environment through EFCM manager using SAN Navigator. Attached and managed HBA configuration. Manage the onsite and offsite automation of tapes. Evaluated the amount media needed to support existing and new applications. Managed the scheduling, policies and the retention time of backups. Managed the amount of current licenses and available license and free cell usage. Large Systems Engineer IBM Corporation Poughkeepsie 1997 to 2001

Account (Enterprise Environment) primarily responsible for the post sale maintenance of IBM and other vendor hardware and software in customer accounts. Assigned account-level responsibilities to provide accounts with total account systems support. Acted as the primary technical interface to customers for hardware and software technical and operational support, and for the delivery of services as required by the customer. Used advanced technical expertise to conduct problem analysis and problem solving to identify and resolve complex system-level hardware, software and/or operational situations across the customer account. Provided technical assistance and account management advice to less experienced personnel. Planned for and execute hardware services activities and assisted in software services activities including systems assurance, installation planning, account management, systems-level problem determination, installations, discontinuance, and relocation, diagnosis, for IBM and non-IBM systems. Acted as the local technical expert for complex hardware situations. In general, assume the responsibility for developing positive relationships with customer management and staff to ensure a high level of overall customer satisfaction in all assigned accounts. Specifically, ensured a high level of customer satisfaction with IBM technical support and operational services for the customer account(s). Responsible for the technical value relationship by providing expertise to protect revenue base and identify new services opportunities. Education InfoSec Institute October 2018 MS in Information Systems Marist College 2012 to 2014 MBA in Information Security Jones International University 2010 to 2013 B.S in Organizational & Leadership Marist College 2006 to 2008 Skills Mitigation, Remediation, Cdl, Linux, Security

Name: Gabrielle Myers

Email: guerramichelle@example.org

Phone: (897)455-8834