IT Security Analyst IT Security Analyst IT Security Analyst - Allstate Insurance Company Work Experience IT Security Analyst Allstate Insurance Company - Irving, TX January 2019 to Present Ensure the strategic alignment of information security with business strategy to support organizational objectives. Identify and recommend appropriate measures to reduce potential impacts on information resources to a level acceptable to senior management. Lead programs to assess, prevent, and mitigate risk. Integrate security risk reporting and management activities into Allstate day to day processes. Define, monitor, and report on a set of Key Risk Indicators. Participate in risk remediation solution discussions and updates to compliance policy and standards.

Lead or conduct initiatives to ensure that controls and processes are operating effectively. Promote and consult on the positions that help strengthen and secure the organization by either following standards or helping direct others on technology positions. Partner with IT and business partners on security related projects. Lead efforts in developing and implements systems and business control procedures and plans for key areas of the company Lead efforts to develop and implement control procedures, and programs for system and business processes. Develop, implement, document and administer standards and procedures to secure and protect Allstate assets. Respond to and assist with audits, assessments and compliance requests. Serve as client liaison as needed on matters pertaining to Risk Management. Lead and track implementation of enterprise security policies, standards Sr. IT Security Analyst BBVA Compass - Birmingham, AL July 2018 to October 2018 Reference: TREY FINCH) Preparation of security testing checklist to the company Ensure all the controls are covered in the checklist Conducted application penetration testing Conducted Compliance Audits Work independently and manage workload with organization to meet expectations and objectives Develop processes and implement tools and techniques to perform ongoing security assessments of the environment Help standardize processes and procedures and provide improvement Work on multiple projects simultaneously, set priorities and meet deadlines Central tracking and management of enterprise vulnerabilities Keep current with vulnerabilities, attacks, and countermeasures as well as devoting time to research and development activities Implement processes and manage tools used to

identify vulnerabilities and track their remediation within the GM environment Acquainted with various approaches to Grey & Black box security testing Proficient in understanding application level vulnerabilities like XSS, SQL Injection, CSRF, authentication bypass, weak cryptography, authentication flaws etc. Performed scoping engagements, vulnerability assessments, web application penetration testing, network penetration testing, and phishing campaigns to test security controls and policies. Engaged clients in the financial industry of mortgage & finance, information technology software and hardware, IT services, and other professional services Actively search for potential security issues and security gaps that are beyond the ability of detection by any security scanner tool. Initiate and develop new mechanisms to addresses unidentified security holes & challenges. Real-time Analysis and defense. IT Security Test Engineer/Penetration Tester Bank Of America - Charlotte, NC November 2017 to March 2018 Reference:RICK MILLER) Performing web application security testing for Bank owned internal and external applications manually using the help of Proxy tools like BURP SUITE, SSLYZE, and SOAP UI. Verifying the security posture of the applications with respect to OWASP TOP 10 vulnerabilities. Understanding the functionalities of the application to perform Business logic test and verifying all the sensitive information is properly protected. Identified High Severity issues like SQL INJECTION, XSS, CSRF, Missing Functional Level Access Control, and SSL/TLS related issues etc. Reporting the identified vulnerabilities with detailed description about the issues, step to reproduce the issues and its countermeasures. Scheduling the report out calls with application managers and helping them understanding the reported issues. Helping the application team in fixing the issues using the technology specific inbuilt security features if any. Work with internal business units to drive secure configurations in images used for desktops, servers, network devices, and wireless network devices A working knowledge of vulnerabilities and configuration settings and their exploitation in order to gain access to networks, applications, hosts, and desktops Work with computer operations to define standard operating system builds and configurations and develop effective build maintenance processes Develop and maintain server software inventories and manage application whitelisting solutions Knowledge of and familiar with identity and authentication management and their architecture

Provide all assigned responsibilities as part of an on-call rotation Provide recommendations on improving the security posture of the client's enterprise Interacting with the team and helping them if they come across any challenges during the assessment. Helps the application team in understanding the importance of implementing secure SDLC to avoid any disturbances during release. Penetration Tester PGE - Portland, OR January 2016 to October 2017 Conducted security assessment of PKI Enabled Applications. Skilled using Burp Suite, Acunetix Automatic Scanner, NMAP for web and mobile application penetration tests. Acquainted with various approaches to Grey Black box security testing. Proficient in understanding application level vulnerabilities like XSS, SQL Injection, CSRF, authentication bypass, weak cryptography, authentication flaws etc. Actively search for potential security issues and security gaps that are beyond the ability of detection by any security scanner tool. Initiate and develop new mechanisms to addresses unidentified security holes and challenges. Performed Network scanning using tools Nessus, OpenVAS and NMap. Metasploit, Burp Suite, NMap tools were used as part of the penetration testing, on daily basis to complete the assessments. Automation scanning and analysis on the Networks and Applications on a daily basis. Uncovered critical vulnerabilities at the infrastructure level for enterprise networks Vulnerability assessment (VA), Security policy, and network and security audit. Configuration and management of Cisco IDS, Checkpoint firewall. Good knowledge of network and security technologies such as Firewalls, TCP/IP, LAN/WAN, IDS/IPS, Routing and Switching. Monitor, Analyze and respond to security incidents in the infrastructure. Investigate and resolve any security issues found in the infrastructure according to the security standards and procedures. Monitor, Analyze and respond to security incidents in the infrastructure. Investigate Make sure the mobile applications should follow the OWASP Mobile Application Security Verification Standard (MASVS). Good experience in Web technologies like HTTP, HTML, CSS, Forms, Database Connectivity. Training the development team on the most common vulnerabilities and common code review issues and explaining the remediation. Good knowledge in programming and scripting in .net, Java. Ensuring SDLC to be a Secure SDLC. Penetration Tester PayPal - San Jose, CA February 2015 to November 2015 Black box pen testing on internet

and intranet facing applications. Training the development team on the secure coding practices. OWASP Top 10 Issues identifications like SQLi, CSRF, and XSS. Preparation of risk registry for the various projects in the client. Providing details of the issues identified and the remediation plan to the stake holders. Grey Box testing of the applications. Verified the existing controls for least privilege, separation of duties and job rotation. Penetration testing of the applications and APIs to identify the OWASP Top 10 vulnerabilities and SANS 25. Documented information security guidance in step by step operational procedures. Performed threat analysis on the new requirements and features. Assisting in preparation of plans to review software components through source code review or application security review. STRIDE assessment of the applications during the design phase, identifying the threats possible and providing security requirements. Involved in a major merger activity of the company and provided insights in separation of different client data and securing PII. Identification of different vulnerabilities of applications by using proxies like Burp suite to validate the server side validations Identified issues on sessions management, Input validations, output encoding, Logging, Exceptions, Cookie attributes, encryption, Privilege escalations. Jr. SECURITY TEST ENGINEER SIERRA ATLANTIC - IN June 2012 to December 2014 Perform threat modelling of the applications to identify the threats. Identify issues in the web applications in various categories like Cryptography, Exception Management. Worked on installation, configuration, and administration and troubleshooting of LAN/WAN infrastructure. Risk assessment on the application by identifying the issues and prioritizing the issues based on risk level. Collaborate with team members to audit the application prior moving to production. Provided detailed reports based on the findings obtained from the manual and automated testing methodologies, also provide the necessary remediation for individual findings. Attended meetings with Risk assessment team to discuss the previously submitted repor on the findings to ensure that the fixes are made to those applications. Provide explanation of the security requirements to the design team in initial stages of SDLC to minimize the efforts to rework on issues identified during penetration tests. Providing remediation to the developers based on the issues identified. Revalidate the issues to ensure the closure of the vulnerabilities. Verify if the

application has implemented the basic security mechanisms like Job rotation, Privilege escalations, Lease Privilege and Defense in depth. Using various add on in Mozilla to assess the application like Wappalyzer, Flagfox, Live HTTP Header, Tamper data. Education Masters of Science in Engineering Trine University - Angola, IN Bachelor of Information Technology in Information Technology Gitam University Skills SECURITY, METASPLOIT, NESSUS, NMAP, PCI, PROXIES, WIRESHARK, MYSQL, ORACLE, SQL, NETWORK SECURITY, .NET, C#, PERL, PYTHON, SCRIPTING, SWIFT, JAVA, LINUX Additional Information TECHNICAL SKILLS: Standards & Framework OWASP, OSSTMM, PCI DSS Application Scanners IBM Appscan, HP Webinspect ,Acunetix. Network Security Tools Nessus, OpenVAS, NMap Proxies/Sniffers/Tools Burp Suite, Web scarab, Wireshark, idler DirBuster, Veracode, Checkmarx Operating Systems Windows, RHEL, Kali Linux Databases MySQL, MS SQL, Oracle Penetration Testing Wireshark, Metasploit Framework Languages C, C#, Java, Python, Perl, Java scripting, Swift, Obj-C ,.Net, Sai Teja Jampani

Name: Nicole Craig

Email: monicajohnson@example.com

Phone: +1-512-293-1485x4127