IT Security Analyst IT Security Analyst IT Security Analyst - La-Z-Boy Illinois An Information Security professional with around 6 years of experience in Compliance and Risk Management Framework (RMF), Information Security and Assurance, System Development Life Cycle (SDLC), Security Control Assessment, Vulnerability Assessment and Penetration Testing. Knowledge of best practices in monitoring, troubleshooting and resolving issues related to maintenance of network systems. Adept in the usage of Vulnerability Detection/Management Tools and Penetration Testing tools -Wireshark, Acunetix, Qualys, Nessus, Burp Suite, Metasploit, Qualys guard and Nmap. Solid understanding of security threat environment relative to computer network architectures, designs, topologies, applications, databases, email systems, remote access, and operating system platforms. Comprehensive knowledge on Firewalls, LAN/WAN, IDS/IPS, Routers and Switches. Good understanding of PCI DSS compliance, PKI, Privileged Access Management, Data Loss Prevention and Cryptographic Protocols. Hands-on experience in performing Application Security Risk assessments throughout Software Development Life Cycle Facilitating business objectives through the identification and promotion of solutions and innovation. Experience in capturing Critical, High, Medium and Low Vulnerabilities in the applications based on OWASP Top 10 Vulnerabilities and prioritized them based on the criticality. Extensive experience in using Kali Linux to do web application assessment using tools like DirBuster, Nikto and Nmap. Exceptional ability in identifying flaws like SQL Injection, DoS and DDoS Attack, Cross Site Scripting (XSS), CSRF, Path Traversal. Extensive experience in performing SAST (Static Application Security Testing/White-Box Testing) and DAST (Dynamic Application Security Testing/Black-Box Testing) Strong platform knowledge including Microsoft Windows and Unix/Linux Operating Systems. Proficiency in SQL, PL/SQL, NoSQL, Shell Scripting, C, C++, Java, HTML and CSS. Team player with excellent communication (verbal & written), problem solving and interpersonal Skills. Capable of effectively prioritizing and executing tasks independently Work Experience IT Security Analyst La-Z-Boy - Monroe, MI May 2018 to Present Responsibilities Collaborated with Application Development and Release teams in integrating Veracode Scans as part of the CI/CD process. Managed and Implemented Symantec Endpoint Protection system all Production and

Non-Production Servers and Client PCs. Performed risk assessments to help create optimal prevention and management plans. Developed security strategy and performing IT risk assessment, vulnerability assessment and working with the business to mitigate risks. Responsible for providing NASA Glenn Research Center (GRC) risk posture based on GRCSystem.

Strong knowledge on QualysGuard and Qualys suite with Vulnerability Management and Web Application Security. Identifying flaws and weaknesses in information systems that may be exploited to impact the confidentiality, integrity and availability of a system. Update with the new hackings and latest vulnerabilities to ensure no such loopholes are present in the existing system. Planning, Scheduling, tracking and reporting on manual/automated security testing on the internet and intranet applications Security assessment of online applications to identify the vulnerabilities in different categories like Input and data Validation, Authentication, Authorization, Auditing & logging. Defined the security program and integrated application security throughout all phases of Software Development Life Cycle (SDLC) from Requirements Gathering to Testing. Performed security code review of JAVA, .Net, PHP code using static code analysis tools e.g. HP Fortify and IBM AppScan. Help team to remediate security issues with sample code. Monitored and Analyzed network traffic, Intrusion Detection Systems (IDS), security events and logs. Implemented and managed vulnerability management solution using tenable security center, policy compliance, nessus scanners and nessusnetwork monitor. Scripted penetration testing such as vulnerability scanning, network scanning, Codeinjection. Used Sqlmap and Nmap for VAPT, and prepared reports for audit according to OWASP with all issues and their mitigation Tools: Acunetix, Burp Suite, Nmap, Nessus, Application Firewall, WebScarab, HP Web Inspect Penetration Tester Wal-Mart - Bentonville, AR May 2016 to April 2018 Responsibilities: Conduct the IT Risk Assessment and documented key controls. Effectively transform traditional Certification and Accreditation (C&A) programs into a six-step life cycle process consisting, Categorization of information systems, Selection of security controls, Implementation of security controls, Assessment of security controls, Authorization of information systems, Monitoring of security controls Develop, review and evaluate Security Plan based on NIST Special Publications 800-18. Investigates

possible security breaches identified through review of audit reports and Follow-up accordingly with departments / management Prepare and review C&A package for Information Systems. Assessed System Security Controls using SP 800-53A Develop POA&M (Plan of Action & Milestones) document to take corrective actions resulting from ST&E (System Test & Evaluation) Assess program and security controls using Organization IT Security Policy Handbook and NIST Special Publications to provide information necessary to determine their overall effectiveness. Perform Contingency Plan Test and Training to ensure systems recoverability as defined in IT systems security requirements. Environment: Nmap, Nessus, Burp suite, Sqlmap, Dirbuster. Security Analyst (Consultant) Google, Inc. MAPS Division January 2013 to January 2015 India Responsibility: Conducted Network Vulnerability assessments using tools to evaluate attacks, identify system vulnerabilities and develop remediation plans and security procedures. Performed Penetration and Vulnerability assessment and review using Qualys, NMap, Nessus, Metasploit and other tools. Performed network traffic analysis using raw packet data, network flow, Intrusion Detection Systems (IDS), and custom sensor output from communication networks Assisted Application Developers in remediating issues with Security Assessments with respect to OWASP standards. Assisted with the development of processes and procedures to improve incident response times, analysis of incidents, and overall SOC functions. Education Bachelors in Computer Science Engineering JNTU Skills NESSUS (5 years), NMAP (5 years), SECURITY (5 years), QUALYS (3 years), METASPLOIT (2 years) Additional Information TECHNICAL SKILLS: Languages: C, C++, Java, SQL, HTML& CSS, Shell Scripting, JavaScript Tools: Nessus, NMap, Burp Suite, tcpdump, Network Simulator 2, Web Scarab, Wire Shark, DirBuster, Qualys, IBM App Scan Enterprise, AppScan for Source Analysis, , HP Web Inspect, Skills: Pen Testing, SAST, DAST Methodologies: OWASP, CVE, BSSM IDE MS Visual Studio, NoSQL Booster, NetBeans, Eclipse Compliances: HIPAA, PCI, PHI, PCI DSS Databases: MongoDB, IBM DB2, MS-SQL Server, MySQL, Oracle Operating System: Windows P/7/8/10, Unix (Oracle/Sun Solaris) /Linux (RedHat and Debian platforms), Kali Linux, Windows Server 2012 R2, 2016. Network and Application layer Security and Vulnerability tools: VeraCode, Nessus, Knowb4, Wireshark, OVAS,

Cain & Abel, Oracle 12c, EBS, Kali Linux, MBSA, Metaslpoit, Nmap, Vometric. Rapid7 IVR, Metasploit Pro, Retina Network Security Scanner, Fortify, nmap/zenmap, Symantec, McAfee Policy Auditor, Vulnerator, Sailpoint, CyberArk, HP ArcSight.

Name: Donald Davis

Email: jacquelineanderson@example.com

Phone: 680-583-3854