**Summary:**

* Over 7 Years of professional Experience in Vulnerability Analysis focused on performing technical activities on Web Applications, Servers and cloud Infrastructure.
* Skilled and experienced in using Vulnerability management tools like Burp Suite, Wireshark, Metasploit, Nessus, Nmap, Qualys and IBM Appscan.
* Expertise in working on prioritizing scan findings and make recommendations to stakeholders and application teams on remediation activities.
* Integrate vulnerability Management and patching into existing CI/CD.
* Conduct baseline scans to identify gaps and determine the high-risk vulnerabilities of the organization.
* Vulnerability Assessments includes analysis of bugs in various applications, domains, devices, servers by using both manual and Automation tools.
* Document Identified vulnerabilities and work with various teams to fix/remediate in a timely manner.
* Having Good knowledge in gathering requirements from stakeholders, devising and planning and strong technical understanding of vulnerabilities.
* Proficient in Windows/Linux, Unix operating system configuration, utilities and programming.
* Performing Server Hardening Audits which includes OS, Database, and Web Servers
* Experience in using Kali Linux to do web application assessment with tools like Dirbuster, Nikto, and Nmap
* Configured and implemented Azure Virtual networks and VM’s per requirements form the client.
* Good knowledge on Firewalls, IDS, endpoint protection, encryption, malware and attacks.
* Perform security assessment based on OWASP framework and Reporting the identified issues in the industry standard format.
* Strong analytical, problem solving and communication skills.
* Ability to work in large and small teams as well as independently.
* Experience with industry standard frameworks, best practices, and compliance regulations (ISO, NIST, PCI, SOX, etc.)

**Skills:**

IBM AppScan, Wireshark, Kali Linux, SIEM, Nessus, Web Scarab, HP Fortify, Nmap, Burp Suite Pro, Mobile Apps, Metasploit, Splunk, Fiddler, Web Applications, HP WebInspect, Android Tamer, OWASP, Telnet, Certified Ethical Hacker(CEH), Protocols/Standards/Systems: TCP/IP, UDP, Apache server, SSL/TLS, LDAP, HTTP(S), DNS, EAP (TLS, TTLS, MD5), and STRIDE / DREAD threat models. NIST SP 800, SOX

**State of MA-DOR; Chelsea, MA Sept 2016 – Present**

**Security Engineer**

* Performed Unauthenticated / Authenticated web application scans using IBM AppScan standard. Worked closely with developer to mitigate vulnerability findings from Gray Box, White box and manual penetration testing. Execute AppScan and verify reported vulnerabilities with Burp Proxy
* Configured and implemented Nessus security center to perform vulnerability scans on network and infrastructure components. Analyzed and prioritized scan findings for patching. Automate Vulnerability scans with CI/CD pipeline
* Document vulnerability findings and worked with Development and Infrastructure teams till they are remediated/fixed. Communicated vulnerability findings and overall security posture to leadership.
* Design, configure, administer, and document firewall infrastructure. Manage the firewall deployment, rules migrations, and firewall administration.
* Utilized Azure Security center to monitor security status of Network and resources hosted on cloud these include managing ports on VM, scanning container images and review security center recommendations.
* Executed daily vulnerability assessments, threat assessment, and mitigation and reporting activities in order to safeguard information assets and ensure protection has been put in place on the systems.
* Perform vulnerability scans using Nessus Security Center. Assigned roles and permissions to user and department staff. Conducts Pre-assessment and Post assessment activities for assigned systems.
* Maintain spreadsheet for all Applications and Systems. Knowledge of common application vulnerabilities, current threat vectors and mitigations. Identify security risks, threats and vulnerabilities of networks, systems, applications and related components.
* Conducted vulnerability assessment on the application & infrastructure using tools like Kali, Dirbuster, Nmap

Environment: Java, Oracle, TOAD, Nessus, IBM AppScan Source and Standard, Burp Suite Pro, Fiddler, F5, Azure

**Catholic Health Initiatives; Denver, CO July 2013 – July 2016**

**Security Analyst**

* Performed vulnerability assessment on the web application using commercial tool along with added vulnerabilities identified in manual testing.
* Expertise in analyzing threats and categorizing them based on criticality of the security vulnerability
* Involved in scoping, identification, analysis and evaluation of application security risk.
* Evaluated vulnerabilities identified due to configuration issues, patch management and third-party applications
* Involved in detection & classification of vulnerability based on OWASP Top Ten methodology.
* Work on common vulnerabilities such as directory traversal, parameter manipulation, information disclosure, web server vulnerabilities, buffer overflows, format string bugs, weak authentication & authorization schemes, session management, cookie manipulation and forceful browsing.
* Created content for security/cyber incidents to identify malicious incidents and events in the Security Information Event Correlation engine
* Eliminated False Positives in the tool, identified vulnerabilities and recommended Best Practices for securing the application.
* Scan Networks, Servers, and other resources to validate compliance and security issues using numerous tools.
* Generated the technical reports with proper recommendations, mapping with OWASP category, PCI compliance and provide walkthrough to the developers to fix it.
* Installed, configured & customized Fortify Secure Code Analyzer to assist in Secure Development Process.

Environment: Java, HP Fortify, HP Webinspect, Burp Suite, ZAP, Wire Shark, DirBuster, Nessus, Metasploit, Kali Linux