IT Security Analyst IT Security Analyst IT Security Analyst - Naviz Analytics Bellevue, WA Over 4+ years of professional experience working as a Security Engineer/ Analyst with Highly motivated and proven ability to articulate IT Security business values. Seeking to be a valued team member in an ever-changing environment. I plan to use my skills, both passively and actively to defend against potential cyber threats and gain knowledge of those unknown to us. In-depth knowledge of Web Application Security, Application Security Controls and Validation, Regulatory Compliance and Secure Software Development Life Cycle Worked with global security teams performing application and IT infrastructure Security assessments. Solid experience of Manual Website Vulnerability assessments involving infra & Web Applications. Well versed with various vulnerabilities and attacks in web applications - OWASP top 10, Directory traversal. Hands on using Kali Linux and consistent research on new exploitation tools. Hands on Experience in vulnerability assessment and pen testing using various tools like BurpSuite, OWASP ZAP Proxy, Nmap, and Nessus. Validate the false positives and report the issues. Good experience in Web technologies like HTTP, HTML, CSS, Forms, Database Connectivity Ability to handle multiple tasks and work independently as well as in a team. Effective team collaboration and strong communication skills - written & verbal. Good knowledge in HP ALM, JIRA, Rally. Sponsorship required to work in the US Work Experience IT Security Analyst Naviz Analytics - Bellevue, WA July 2015 to Present Responsibilities: Involved in Security & Compliance Team to ensure Security & Compliance is met or strictly followed within the Organization as per the Industry Standards Defined the security program and integrated application security throughout all phases of Software Development Life Cycle (SDLC) from Requirements Gathering to Testing. Used Burp suite for manual validation like SQL injection, XSS, CSRF. Responsible for manual triage, configuring policies, and also assisting with any technical design issues that arise during this time. Developed Security policies and baselines for web applications. Performed compliance audits to ensure security policies and baselines have been adequately implemented. Risk assessment based on vulnerability reports, recommend & prepare remediation plan to fix identified high vulnerabilities/risks. Provide the report and explain the issues by interface with development team.

Worked with business partners and 3rd party vendors to Implement Infrastructure to apply Qualys Vulnerability Scanning at an enterprise level. Pentesting home lab to learn more tools, exploiting the remote system with advance tools like veil, Nmap, Armitage Website exploitation (Burp Suit, OWASP), host scanning through an own xml script. IT Security Engineer Microsoft Cyber Defense Operations Center - Redmond, WA January 2014 to June 2015 Responsibilities: Incident response of new threat that was reported. Network traffic analysis and packet captures using Wireshark. Used Wireshark to troubleshoot servers that were impacted due to vulnerability data to block the proper ports during vulnerability scan to minimize impact such as air flight delays & Tested for the encryption. Document project, including work flows and operational roles and tasks. Investigation of internal alerts & Performed payload analysis of packets using Wireshark. Track work across programs using Team Foundation Server (TFS). Manage implementation of new services, private networks, access controls, policies and E2E Security processes. Drive the compliance and adoption for threat and vulnerability management with different service engineering and business stakeholders thru implementation of Qualys systems, Security reporting, effective system auditing. Execute and craft different payloads to attack the system to execute XSS and different attacks. Conducts regularly review of Global Security Incidents reports an update to the internal teams. Effectively communicated Security risks and solutions to leadership, business partners and IT staff. Investigation of external reports, including malware analysis as a junior analyst. Education Master's in Project Management Harrisburg University of Science and Technology December 2016 Skills QUALYS (4 years), SECURITY (4 years), NMAP (2 years), TESTING (2 years), WIRESHARK (1 year) Additional Information Skills and Technologies: Operating Systems: Variants of Windows and Kali Linux. Other Tools: Wireshark, Burp Suite, Qualys Vulnerability Management, Qualys Enterprise, Nessus, Nmap, OWASP-Zap, Web Inspect, HP Fortify, Tableau. Independent Study: Penetration Testing, The Web Application Hacker's Handbook, Linux+, PCI/DSS, Security+

Name: Christine Pitts

Email: njohnson@example.net

Phone: 7584950857