Information Security Analyst Information Security Analyst Information Security Analyst - State of Indiana Indianapolis, IN With extensive experience in Network Security, Incident Handling and implementing Security controls at organization, OS, network and application level, seeking a responsible position as an Information or Cyber Security Analyst where I can contribute towards incident prevention, detection/analysis, containment, eradication, recovery and safety of the organization. o Involved in Software development Life cycle (SDLC) to ensure security controls in place. o Experience in Threat Modeling during Requirement gathering and Design phases and experience incident and event handling through multitude of tools. o Experience in comprehensive SIEM infrastructure for monitoring and alerting - Splunk. o Experience in IR process management and handling (Alert Logic). o Experience on vulnerability assessment and penetration testing using various tools like Burpsuite, OWASP ZAP Proxy, NMap, Nessus, Kali Linux, Metasploit, Accunetix o Knowledge performing Application Scan using IBM Appscan o Capable of identifying flaws like Injection, XSS, Insecure direct object reference, Security Misconfiguration, Sensitive data exposure, Functional level access control, CSRF, Invalidated redirects o Experience with TCP/IP, Firewalls, LAN/WAN. o Experience in Linux system administration. o Static Code Analysis during development phase. o CompTIA Security+ certified and A Certified Ethical Hacker (CEH). o A Pen tester with experience of penetration testing on various applications in different tools. o Penetration testing based on OWASP Top 10. o Good team player with excellent communication skills and ability to work independently along with strong problem solving, learning and interpersonal skills. Authorized to work in the US for any employer Work Experience Information Security Analyst State of Indiana - Indianapolis, IN May 2016 to Present Assist and implement several information security process for the client (Sate of Indiana) in the existing team spanning the service line verticals of IT Security, Risk Management, Regulatory Compliance, Digital Forensics, IT Audit, and Re- porting Services. o Vulnerability assessments and Penetration Testing - Performed network penetration tests, scans, and ethical hacking assessments in internal networks, and web applications. o Performed pen testing and discovered security vulnerabilities in various web applications and web services using manual testing and automated tools - IBM AppScan, Sqlmap, Burp Suite and other

tools like Postman Interceptor, Nessus, Nmap, Kali Linux, Metasploit Framework etc, . o Perform Information Security audits and configuration reviews o Discover Software insecurities and stomp out bugs and flaws of the web application that holds valuable PII Data in different forms of Front End and Back End. o Risk Evaluation to client information resources, prioritizing concerns, and developing plans and to remediate risks through multitude of security tools. o Asses and analyze the vulnerabilities on the data base side like SQL Injection, Blind MongoDB, NoSQL Injection and on the back end like Java Script Denial of Service attacks. o Perform threat hunting activities, implement preventative controls in response to new threat intelligence that are received, and assist in the resolution of various security incidents that may arise. o Use SOAP UI to execute testing cases for secure back end validations on different applications of the state. o Other assigned tasks: Quality Assurance duties to test the applications manually, processes by following SDLC methodologies. Technology Support Center October 2014 to May 2016 o Maintained IT infrastructure in transportation department and responsible for office computers and printers. o Troubleshooting computers, applying patches and maintaining up-to-date virus definitions in anti-viruses. o System administration, familiar with Active directory Security Operations Center Analyst Intern Technology Support Center May 2015 to August 2015 o Assisted in internal audits to ensure Networks, Systems and Applications are in compliance with security related regulatory requirements. o Trained in CIRT (Computer Incident Response Team) process. o Participated in numerous computer incident investigations. o Implemented automated security monitoring processes with basic scripts in Python. o Involved in Vulnerability assessments, generating & presenting reports on security vulnerabilities using Nessus. o Worked on real-time detection and reaction services of incidents of information security under process audit. o Parsing and Analyzing the Website Data using CIF - Implemented automated scripts for crawling the web data and analyzed data for finding fixed patterns. Created parsers and analyzed different web data using CIF o Incident Handling and Management through incident management tools it simply needs to connect to the server o CompTIA Security+ CE Boot Camp at IUPUI October 2013 to October 2013 Online Java Compiler Application(JAVA, HTML, CSS) October 2013 Stand-alone application executing

java program and easily compile and debug it online. The client machine doesn't require any JDK installed on it; rather, it simply needs to connect to the server, which executes t h e java code and projects respective errors to client Boot Camp & Training o CompTIA Security+ CE Boot Camp at IUPUI o Ethical Hacking training from B9ITS (EC-Council certified institute) o Network & Web Application Penetration testing - B9ITS Hacking Trainer IT Analyst Intern Vizag Steel Plant June 2012 to January 2013 o 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. o Perform threat modeling of the applications to identify the threats. o Identify issues in the web applications in various categories like Cryptography, Exception Management, client- server side attacks. o Trained in basics of different stages of pen testing Education Master of Science in Computer and Information Science in Computer and Information Science Purdue School of Engineering May 2016 Technology Jawaharlal Nehru Technological University - Hyderabad, Telangana May 2014 Skills Linux (1 year), Metasploit (1 year), Nessus (1 year), Nmap (1 year), Testing (2 years) Additional Information Technical Skills Programming/Networking: HTML, SQL, Python, TCP/IP, DNS, DHCP, Wireshark, Alert Logic IDS. Penetration Testing / Vulnerability Scanning: Burp Suite, Sqlmap, OWASP Mutillidae, Qualys Vulnerability man- agement (Qualys guard), nipper, OWASP Zed Attack Proxy, Nessus, Retina Network Scanner, Nmap, Metasploit Framework, Acunetix Web Vulnerability Scanner, OWASP ZAP, Netsparker Scanner, IBM AppScan. Other Tools: VMware, Virtual box, MS Office and MS Visio, Veracode, Jenkins, Postman Interceptor. Databases: MySql, MS SQL, Oracle Operating Systems: Windows 7/8/8.1/10, Windows Server 2012 R2, Linux (Kali, Ubuntu), Mac OS, Parrot OS.

Name: Alyssa Fowler

Email: catherine61@example.com

Phone: 870-587-1010x2555