Security Analyst Security Analyst Security Analyst South Plainfield, NJ Over 7+ years of infrastructure and security experience with specialization in application security, Data Security and SIEM technologies Strong understanding of OWASP and SANS standards Hands on experience working with tools like Metasploit, Burp Suite, Sqlmap, OWASP ZAP Proxy and IBM Appscan & HP Fortify etc., Conducted white/gray box penetration testing on the financial systems using Kali Linuxfor OWASP vulnerabilities like XSS, SQL Injection, CSRF, Privilege Escalation and all the test-case of a web application security testing Proficient in analyzing different security threats to organizations by identifying the indicators that a security incident is underway, composing and creating security policies and procedures to be followed when an incident is detected, and investigation methods use to collect evidence for prevention and prosecution. Experience as a privacy/ security analyst, with applicable knowledge of regulatory compliance procedures related to PCI Perform Vulnerability assessment and policy compliance and PCI compliance using Qualys and IBM App scan Provide consultative support with implementation of remediation steps, standards, and best practices. Recommended and Implemented remediation steps, standards, and best practices. CertifiedinQualys Vulnerability Management Authorized to work in the US for any employer Work Experience Security Analyst AIG Insurance - Dallas, TX June 2015 to July 2016 Worked extensively on SIEM, IDS/IPS, log management, network security infrastructure Identify, design, and develop new methods for incident detection and intelligence collection of anomalous behavior, system and network patterns, and potential breaches Monitor, and analyze offense and events generated on federal platform with an immediate and appropriate actions to verify offense Reconciled assets to log sources from Qradar to identify assets that are and are not sending logs to Qradar. Created asset groups and asset profiles for federal environment Identified configuration changes that would improve overall utilization of the SIEM Test the applications & infrastructure using Kali Linux& other security tools Implemented Tenable Nessus, and customized audit compliance dashboards of system configurations and content for the Vulnerability / Configuration Compliance Management and Monitoring Programs. Perform threat and risk analysis to the company infrastructure to facilitate effective incident response, and the creation of new security

opportunities Develop historical threat activity through aggregation, correlation and trending to predict future threats Maintained standard operating procedures, processes and guidelines Analyze systems for potential vulnerabilities with the help of Qualys VM that may result from improper system configuration, hardware or software flaws Ensure compliance with policies, procedures, and regulations (i.e. PCI DSS) Security Consultant Austco - Dallas, TX October 2014 to May 2015 Served as the primary responder for managed security incidents pertaining to client firewalls and all network infrastructure components Monitored SIEM and IDS/IPS feeds to identify possible enterprise threats. Investigate and triage threats to determine nature of incident Monitored SIEM and IDS/IPS feeds to identify possible enterprise threats.Investigate and triage threats to determine nature of incident. Forwarded findings to Cyber Forensic Investigations or Security Incident Response teams to further investigate and re mediate findings helped to research open-source intelligence feeds for current and emerging threat information Ability to conduct manual Penetration Tests on sensitive systems. Utilized tools such as NMAP, Nessus, Qualysto accomplish network reconnaissance and surveillance in preparation for exploitation. Assist in engineering integration to other key security systems Create and support security awareness programs to inform and educate employees IT Security Consultant Bajaj Allianz General Insurance Co. Ltd - Bangalore, Karnataka May 2012 to August 2014 Bangalore, India Verified SSL authentication for secure applications development on Web Servers. Performed dynamic and static analysis of web application using IBM AppScan. Investigate and triage threats to determine nature of incident Identify security vulnerabilities and generate reports and fix recommendations using IBM AppScan Helped to research open-source intelligence feeds for current and emerging threat information Conducted white/gray box penetration testing on the financial systems using Kali Linux for OWASP top 10 Vulnerabilities like XSS, SQL Injection, CSRF, Privilege Escalation and all the test-case of a web application security testing Utilized tools such as NMAP, Nessus, Qualys, and Nexpose to accomplish network reconnaissance and surveillance in preparation for exploitation. Assist in engineering integration to other key security systems Create and support security awareness programs to inform and educate employees System Admin Vibertech Solutions

Pvt. Ltd - Bangalore, Karnataka June 2009 to April 2012 Bangalore, India Installation and Configuration of Linux systems like Red Hat and Windows Servers. Also involved in user account management Actively involved in Monitoring the server's health status using different tools Responsible for application support on Red Hat servers which included apache configurations Experience working with Storage Area Network (SAN). Experience in Performance monitoring, usage and load the system, changing kernel parameters for better performance. Worked with Perl, Shell Scripting (ksh, bash) to automate administration tasks. RPM package installation & upgrade released by Red Hat in the repository Administration of client machines using SSH and FTP Supported for application upgrade and rollback, Start or Stop services in Linux Servers. Education Bachelors of Technology in Technology Jawaharlal Nehru Technological University 2009 Additional Information TECHNICAL SKILLS: Operating Systems Microsoft: Server 2003/Server 2008 Linux: CentOS, Red Hat, Fedora, Ubuntu Server/Desktop, Kali Linux OWASP/SANS Vulnerability XSS, SQL Injection, CSRF, Security Misconfiguration, Sensitive Data Exposure, Insecure Direct Object Reference IDS/IPS McAfee Intrushield / NSM, McAfee e-Policy Orchestrator (ePO) Web Technologies HTML, Java Script, Java, Microsoft.Net SIEMs IBM QRadar, Splunk Security Tools IBM AppScan, Qualys, Wireshark, Snort, Tcpdump, Tcprelay, Nmap, Netcat, Iptables, Malwarebytes, Nessus, SQLmap, Burp Suite Networking and concepts Ethernet, LAN/WAN/MAN, TCP/IP, DNS, DHCP, FTP, TELNET, SMTP, POP3, SSH, UDP, ICMP, IPsec, HTTP/HTTPS, Network Topologies, Firewalls, VPNs

Name: David Perkins

Email: christineking@example.org

Phone: 759.473.1745x4020