IT Security Analyst IT Security Analyst IT Security Analyst - Dollar General Corp Indianapolis, IN Over 6+ years of infrastructure and IT security experience with specialization in Data Security, application security, and Information Security in Systems Development Life Cycle (SDLC), security life cycle and vulnerability management using various security standards. Proven enterprise experience in security management, aptitude for good customer service, leadership, and excellent communication and presentation skills. 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. Strong Knowledge in endpoint security and security incident remediation. Ability to interact with various teams to support security assessments and continues monitoring for clients. Provided consultative support with implementation of remediation steps, standards, and best practices. Good knowledge and experience in Designing and Implementation of SIEM tools (Splunk and Qradar) and creating Policies Strong knowledge and hands-on experience in performing various admin activities with AV agents and Consoles Expert in performing admin and operations for endpoint. Certified in Qualys Vulnerability Management, Training for COMPTIA Security+, CISSP Authorized to work in the US for any employer Work Experience IT Security Analyst Dollar General Corp - Goodlettsville, TN January 2017 to Present Performs application vulnerability assessment using static code analysis techniques using Microfocus fortify. Install and configure Fortify tools (SSC and SCA) upon the organization requirements. Works within the security team, performing application vulnerability assessments on corporate applications to ensure proper development and secure implementation. Manage Application security vulnerability management process trough Micro Focus SSC and coordinate with respective teams. Identify and analyze the false positives from the test results and triage the issues into critical, high, medium and low categories. Assist Application development teams with understanding vulnerabilities and remediation strategies. Create standard procedural documents for Micro Focus fortify and Static code analysis process and Implementation of SSC in the Application Security Process. Assist Developers in using Micro Focus Fortify.

Create Shell and Ruby Scripts to perform SCA scans after hours Collaborates with software development teams to design secure software systems. Internal teams coordination with log Management activities using SIEM tools: QRadar and Splunk. Worked on McAfee Anti-Virus 8.8 and ePO 5.9 console Performed Admin Operational activities on Cylance - Using SCCM for software deployments Gathered information from other IT and non- IT staff to obtain information regarding security problems to networks, endpoints, and applications Assisted with the development and maintenance of technical documentation, field guides, and Standard Operating Procedures (SOP) Monitor, and analyze offense and events generated on federal platform with immediate and appropriate actions to verify offenses. Participated, as needed, in security product implementation reviews Security Consultant RCI - Dallas, TX June 2014 to Present 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. 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, Qualys 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. Security Analyst AIG Insurance - Dallas, TX June 2015 to December 2016 Worked extensively on DLP, SIEM, IDS/IPS, log management, network security infrastructure and Vulnerability Management. Identify, design, and develop new methods for incident detection and intelligence collection of anomalous behavior, system and network patterns, and potential breaches. Upgrade Symantec DLP version 15.0, 15.0.1 MP1, and 15.1. Installed and configure Enforce Server Administration console to manage Endpoints, policies, policy rules, Agent groups, Incidents, manage DLP servers, and etc. Installed and Configure Endpoint Prevent and Discover detection server to protect Data in use. Installed and Configure Network Discover server to discover data at rest and Configure

Network protect to protect data at rest by Quarantine, Copy and Encrypt data. Performed vendor File share scan with Symantec DLP by setting up Site-to-site VPN. Configure AD with Enforce Server to assign appropriate policy to agent groups. Create connection to LDAP servers, Configure Active directory server connection, and schedule directory server indexing. Configured, monitored, and maintained security compliance of all company endpoints using Symantec Design and Implemented McAfee agents in multiple environment's and OU's Perform administrated and operational activates on Sophos AV Completed project to force encryption of all USB and CD / DVD media attached any device within the company, using TrendMicro Endpoint Encryption Software. Implemented Symantec DLP in monitoring, warning and blocking mode. Monitor, and analyze offense and events generated on federal platform with immediate and appropriate actions to verify offense. Reconciled assets to log sources from Splunk to identify assets that are and are not sending logs to Splunk. Scanned a variety of applications to find the vulnerability according to the organization standards and rechecked it with the help of Qualys VM. Analyze systems for potential vulnerabilities with the help of Qualys VM that may result from improper system configuration, hardware or software flaws. IT Security Consultant Bajaj Allianz General Insurance Co. Ltd - Bengaluru, Karnataka May 2013 to December 2013 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 - Bengaluru, Karnataka June 2012 to April 2013 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 Master of Science in Computer Science and Information Systems University of Michigan USA 2015 Bachelors of Technology in Technology Jawaharlal Nehru Technological University India 2012 Skills IDS (2 years), IPS (2 years), Qualys (3 years), Security (5 years), Splunk. (3 years), access, HTML, training, Active Directory, testing Additional Information SKILLS Operating Systems Microsoft: Server 2003, 2008, 2012 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) DLP Symantec Programming languages C#, .Net, JA V A, PYTHON Web Technologies HTML, Java Script, Ruby, Shell, CSS, HTML, PHP, PERL Endpoint Protection Cylance, Symantec, McAfee Encryption Symantec IDE's Visual Studio, Eclipse Application Servers Apache Tomcat, IIS SIEMs IBM QRadar, Splunk Application Security Tools Microfocus Fortify, Web Inspect, IBM AppScan Antivirus McAfee Other Security Tools Burp Suite, Wireshark, Snort, Tcpdump, Tcprelay, Nmap, Netcat, Iptables, Malwarebytes, SQLmap. Vulnerability Management Qualys, Nessus 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: Kim Horne

Email: austinnicholas@example.net

Phone: 001-427-698-5259x7425