IT Security/Vulnerability Assessment Analyst IT Security/Vulnerability Assessment Analyst IT Security/Vulnerability Assessment Analyst - BNY Mellon, NY Princeton, NJ With over 7 years of extensive experience in Information and Technology which includes involvement in Administrating, Monitoring and Developing various applications as a Web Application Administrator, IT Security/Vulnerability analyst and A Certified Ethical Hacker V.9 Authorized to work in the US for any employer Work Experience IT Security/Vulnerability Assessment Analyst BNY Mellon, NY April 2018 to Present Performs daily operational monitoring, analysis and reporting of security events from multiple Security Information Monitoring tools and methods for malicious or suspicious activity.

Plan, develop, and execute vulnerability scans of organization information systems. Provide critical analyses and information from vulnerability data, which can be leveraged to enhance the security of our products. Manage tracking and remediation of vulnerabilities by leveraging agreed upon action plans and timelines with responsible technology developers and support teams. Generate reports on assessment findings/patch compliance and summarize information to facilitate remediation tasks and able to Identify and resolve false positive findings in assessment results. Acts as technical advisor to recommend solutions for project managers, analysts, system development resources, and trainers Provides risk mitigation recommendations and works with technology and business partners to help mitigate technology risk observations Assisting stakeholders with recommendations to address key control deficiencies Works with LOB representatives to ensure remediation efforts adhere to corporate policies. Tracks, coordinates, and resolves issues identified in and related control, compliance, or risk work. Monitor Access Management activities to ensure segregation of duties. Monitoring of computing platform compliance with security policies and directives. Tools: Qualys, Nessus, Archer, IBM Qradar, Splunk. Security Analyst Guardian Life Insurance Of America August 2016 to April 2018 Performed internal/external vulnerability scanning of the application and network using various tools Qualys, Nessus. Reported and recommended the vulnerabilities fixings for future vulnerability prevention. Assembled data classification, data flows, port scans, application penetration test results, vendor responses, network diagrams for application reviews. Represented application teams when

security questions arose regarding their applications. Tested applications for security vulnerabilities (including web applications on Apache and IIS servers and their XSS, CSRF and other vulnerabilities) using common network vulnerability assessment tools. Worked with application teams to evaluate risk and mitigate vulnerabilities. Actively responded to automated responses to disable user accounts, kill processes, restart or stop services, force user log-off, and block IP addresses. Aggregate, correlate, and analyze log data from network devices, security devices and other key assets using Qradar System performance and health monitoring of Qradar (Created a SIEM Webpage using VBScript on IIS Server). Create and Run Qradar Searches for Rules and Reports. Technical representation for PCI, CPM and SOX Audit Review and monitoring Coordinated security patch evaluation, testing, and implementation and monitoring. Application Security Analyst Verizon Wireless - Piscataway, NJ August 2015 to June 2016 Use the following Intrusion Prevention Tools to deter incidents (Websense, Palo Alto, Tipping Point, and FireEye) Utilizes the Kali OS to execute attacks and testing for various entities. Assisted in the information gathering and reporting phase of the assessment. Developed threat models for unintentional insider threats and social engineering attacks against applications. Gathered pattern analysis data for various insider threat teams for consultation purposes. Produced analysis and briefings on current events that pertained to intentional and unintentional insider threat topics Validate security access requests Extensive use of analytical and problem solving skills to determine End-Users security related issues. Executed block enrollment batch process, and batch for adding/removing users from academic groups and removal of service indicators. Remediate and investigate any US-CERT emails. Disable user/RSA accounts due to infections or malicious activity. Administrator for Sidewinder Firewalls Cigna - Philadelphia, PA August 2014 to June 2015 Philadelphia Aug'14 - June'15 Application Server Support Provided support to Development, Testing, Staging and Production, environments. Created Weblogic domains, Managed servers, Clusters, machines and start up scripts. Configured JDBC resources, data sources and bounded to the J2EE applications, configured the connection pools for the data sources Involved in doing a performance benchmark of Weblogic server by using Load runner. Created WLST, ANT scripts, and shell scripts to

automate the deployment process. Involved in creating and configuring the Clustered platform domain for load balancing and fail over Involved in developing controls like EJB Controls, JMS Controls, DB Controls by using Weblogic Workshop IDE. Deployed various WAR, JAR, EAR applications in clustered environment with automated process. Administrator for Sidewinder Firewalls (McAfee Enterprise Firewalls), Checkpoint and Checkpoint NG. Responsible for administration and maintenance of RSA Authentication Manager5.X and 6.1. Responsible for administration and maintenance of 8e6 Technologies' R2000 and R3000 Content Filter. Responsible for vendor relations and evaluating new security products. Configured SSL for data encryption and client authentication and two Way SSL for Weblogic using Key tool. Good knowledge in using the Jenkins, Accurev for the source code controlling. Environment: Weblogic 11g, SQL developer, SiteMinder, Jenkins, Accurev, JDK1.5, TLS 1.3, HP ALM. Application Server Administrator United Health Group - Horsham, PA September 2012 to December 2012 Performed Web Logic Server administration tasks such as Installation, Configuration, Monitoring and Performance Tuning of WebLogic Server 8.1/9.2/10gR3/11g. Installed, configured and administered PEGA BPM 5.6/6.0. Configured Apache 2.2 on different physical and virtual boxes in various environments to handle the static content. Configured and worked with Apache SSL modules in the process of installing SSL certificates on to the Web and Application servers. Dealt with troubleshooting issues like Out of Memory, High CPU, Server Hang and Database related issues. Configured Node Manager to remotely administer managed servers. Managed and monitored JVM Performance by adjusting WebLogic heap size and garbage collection parameters. Analyzed server performance data and identified all sources of problems and recommended courses of action to increase performance. Provided 24/7 on call production support with the Development, Test and Production teams. Environment: WebLogic Server 8.1/9.2/10.3/11gR1, SOA Suite 8.1, Apache 1.3/2.2, Tomcat 5.0/6.0, JBOSS 4.2/5.0, Oracle Fusion Middleware, JDK1.4/1.5/1.6, HPOpenview, Siteminder, WLST, Sun JVM, , Oracle 9i/10g/11g/RAC, JDBC, XML, BMC Remedy. Platforms/Skills Snort, Backtrack, Kali, PGP, Metasploit, Active Directory, ClamWin, ClamAV, Minitab, Wireshark, Virtualbox, VMware, Django Framework, TCPDump, MBSA,

Nessus, NTOP, Log Parser, Splunk, , Bastille, Nagios, LAMP, Volatility Framework, NMAP. Windows XP/Vista/10, Linux, Mac OS Access control, Active Directory Malware analysis. NETWORK MAPPING Remote desktop Monitoring. Virtualization TCP/UDP - OSI Model (4) Ticketing System. LAN/WAN, VPN, IDS/IPS, FIREWALL Web development, word press. Education Bachelor's Skills security, testing, access, Microsoft Office, Active Directory, HTML, Sharepoint

Name: Cindy Abbott

Email: lhernandez@example.org

Phone: 209-708-9332x99584