Senior Specialist - IT Security Operations Senior Specialist - IT Security Operations Senior Specialist - IT Security Operations - Marsh & McLennan Companies Flower Mound, TX Information Security Specialist over 10 years experience in infrastructure testing including hardware and application assessments, source and binary software code review and web application. Automating of manual commands by scripting is a skill used to formulate repetitive tasks. Self motivated with the ability to work with little to no supervision with excellent organizational skills. A demonstrated strong team player with a commitment to customer service. Quick learner enjoys challenge-seeking opportunity to learn and improve proficiency. Committed to the highest level of excellence through achievement. Work Experience Senior Specialist - IT Security Operations Marsh & McLennan Companies January 2017 to Present Threat analysis and malware analysis. Responsibilities include: Monitoring Dell Secureworks Portal for alerts and events and escalating to the appropriate group for analysis. Monitoring FireEye NX and HX alerts and taking appropriate action based upon analysis. FireEye HX acquisition and analysis. Threat Hunting analysis using proxy logs and Log Rhythm. Using Log Rhythm to search and provide analysis of malicious activity. Assisting the Incident Response Team in malware response and analysis. Enhancing and automating monitoring capabilities through the use of Application Programming Interfaces (API's). Information Security Analyst Santander Consumer USA February 2015 to December 2016 Threat Analysis, Incident Response and malware analysis and removal. Review, install and maintain current and new infrastructure security appliances. Responsibilities include: Perform vulnerability analysis and assessment of Enterprise infrastructures and applications using the following technologies: Qualys and Portswigger - Burp Proxy. Black box application testing for OWASP top ten (10) vulnerabilities such as Cross-Site Scripting and SQL Injection vulnerabilities. Work with the Business Units (BU) to ensure applications meet security compliance and guidelines. Security experience with networking technologies including, but not limited to routers, switches, and firewalls. SNORT IDS Administration. Perform application testing within the infrastructure to ensure consistent security requirements are met. Daily maintenance, review and monitoring of AlertLogic and BlueCoat Proxy. Understanding of networking and communication techniques including WANs, LANs, Internet, Intranets, and protocols such as TCP, UDP, and IPSEC. Perform security scans and analysis on internal and external infrastructure and reporting. Analyze and maintain current Domain infrastructure. Security Engineer Copart, Inc May 2014 to October 2014 Perform local and remote malware removal and analysis from within the infrastructure without travel requirements. Review, install and maintain current and new infrastructure security appliances or applications. Responsibilities include: Perform vulnerability analysis and assessment of Enterprise infrastructures and applications using the following technologies: OWASP - ZAP Proxy, Portswigger - Burp Proxy, Cyber Security Software - SQLMap and Rapid7 - Nexpose. Black box application testing for OWASP top ten (10) vulnerabilities such as Cross-Site Scripting and SQL Injection vulnerabilities. Work with the Business Units (BU) to ensure applications meet security compliance and guidelines. Security experience with networking technologies including, but not limited to routers, switches, and firewalls. SIEMS - Splunk Enterprise Administrator. SNORT IDS Administrator. Perform application testing within the infrastructure to ensure consistent security requirements are met. Daily maintenance, review and monitoring of Radware, BlueCoat Proxy, Cisco ACS and Pix Firewall Appliances. Understanding of networking and communication techniques including WANs, LANs, Internet, Intranets, and protocols such as TCP, UDP, and IPSEC. Perform monthly security scans and analysis on internal and external infrastructure and reporting. Analyze and maintain current Domain infrastructure. Malware Engineer Fujitsu North America Corporation January 2014 to May 2014 Perform local and remote malware removal and analysis within the infrastructure without travel requirements. Coordinate with Service Desk tickets for re-imaging of client workstations. Responsibilities include: Perform vulnerability analysis and assessment of Enterprise infrastructures and applications using the following technologies: OWASP - ZAP Proxy, Portswigger - Burp Proxy, Cyber Security Software - SQLMap, Rapid7 - Nexpose and nCircle - IP360. Daily response and monitoring of FireEye Adaptive Defense Alerts. Setup, define and perform scanning of internal and external infrastructure using Qualys Guard. Send monthly reports to management for review of vulnerability analysis. Setup and maintenance of Palo Alto Firewall. Perform application testing within infrastructure when necessary to ensure consistent security requirements are met. Analyze and maintain current Domain infrastructure for Fujitsu. Application Security Consultant OpenSky Corporation January 2013 to April 2014 Perform vulnerability analysis and assessment of Enterprise infrastructures and applications using the following technologies: Burp Proxy, Cyber Security Software - SQLMap. Responsibilities include: Senior Security Engineer Accretive Solutions April 2013 to December 2013 Perform infrastructure and application vulnerability assessments using the following technologies: Rapid7 - Nexpose Scanner, PortSwigger Web Security - Burp Proxy, Cyber Security Software - Nipper, Mesploit Framework and Qualys On Demand Security - Qualys Scan. Responsibilities include: Performing penetration and assessments of client's network, workstations and applications. Baylor Health Care Systems December 2012 to December 2012 12/2012 Enterprise Security Group Performed Threat Analysis, Incident Response and team coordination efforts for the removal of malware from the network infrastructure of workstations and servers. Responsibilities included: Create an Incident Response Team to remove malware from workstations and servers. Analyzed malware and suggest remediation efforts for removal. Assisted in removal of malware from workstations and servers. Information Security Assessment Specialist Security - Burp Proxy, Cyber Security Software March 2004 to August 2012 Focused completely on the security of applications and infrastructure. Perform and coordinate infrastructure and application vulnerability assessments using the following technologies: Tenable Network Security - Nessus Scanner, Rapid7 - Nexpose Scanner, PortSwigger Web Security - Burp Proxy, Cyber Security Software - Nipper, and Mesploit Framework, Qualys On Demand Security - Qualys Scan and IBM Security AppScan Standard. Coordinating and assisted in National Incidents and gather information for distribution of new vulnerabilities. Designs, code, and test automated scripting for group use in penetration testing using Assembly Language, XML, HTML, Javascript, CSS, C, PHP and Perl. Reverse Engineering of binary code using WinDbg, Ollydbg and IDA Professional. Performed computer forensics. Performed Incident Response and team coordination efforts for malware removal. Responsibilities included: Coordinated and performed internal and external penetration testing. Coordinated and performed internal and external Web application assessments. Monitored and analyzed malicious/suspicious network traffic. Analyzed malware and suggest remediation efforts for removal. Assisted in coordination and removal of malware from workstation and servers. Review and analyze Firewall configurations such as Nokia, PIX, Netscreen and Juniper. Federal Reserve Bank of Dallas 1988 to 2012 National Incident Response Team Business Units (BU) 2010 to 2010 vulnerabilities such as Cross-Site Scripting and SQL Injection vulnerabilities. Work with the Business Units (BU) to ensure applications meet security compliance and guidelines. Creating, modifying, proofing and delivery of the finals report to the client. Business Units (BU) 2010 to 2010 Black box application testing for OWASP top ten (10) vulnerabilities such as Cross-Site Scripting and SQL Injection vulnerabilities. Work with the Business Units (BU) to ensure applications meet security compliance and guidelines. Creating, writing and delivery of the final reports to the client. Maintaining Operating Systems, Firewall, Switches and Routers for Security Test Lab. Network Operations/Support Engineer Information Technologies Group February 2002 to March 2004 Maintain internal and external firewalls. Setup and maintenance of Palo Alto Firewall. Installed and maintained Solaris 2.6, 2.7 and 2.8 hosts. Automated Cisco and Unix daily monitoring routines and weekend installations. Created and maintained automated installation packages for current releases of software to adhere to the Information Security Manual (ISM) standards. Responsibilities included: Monitored and analyzed malicious/suspicious network traffic. Coordinated and performed weekly firewall rule changes. Configure and maintain Netscreen Firewall configurations. Data and Communications Installation Technician March 1988 to February 2002 Maintained two factor authentication utilizing RSA SecureID Tokens. Maintained and installed Windows NT and Windows 2000 Server platforms. Install computer hardware, software and troubleshot problem areas. Maintain T1 and T3 Data circuits. Installed and maintained IBM Token Ring and Ethernet Local Area Networks. Maintain Siemens 8000, 9000 ad 9751 CBX and Phonemail Systems. Performed Fiber and Copper splicing and termination. Installed and maintained Cisco and 3Com Routers and Switches. Created Network design, capacity planning, installation/ implementation, and troubleshooting documents for internal use. ADDITIONAL TECHNOLOGIES USED Unix Shell Scripting, Windows scripting, Expect, Terminal Control

Language (TCL), Java, Microsoft Sequel Server (MS-SQL), MYSQL, Visual Basic, Application fuzzing, Microsoft office tools, Microsoft Word, Excel, Powerpoint, Visio. Education High school or equivalent Skills Information Security, Cyber Security, Siem, Network Security, Nist

Name: James Mcdonald

Email: ymccormick@example.org

Phone: 800.708.6864