Enterprise Vulnerability Management- Sr. Security Analyst Enterprise Vulnerability Management- Sr. Security Analyst Security Professional Minneapolis, MN Over 5 years of experience in Information Technology including but not limited to, pentesting, vulnerability management, incident response, IT audit, and regulatory compliance. Deep knowledge of PCI DSS, Center of Internet Security (CIS), hardening, HIPPA/HITRUST, Sarbanes-Oxley (SOX) regulation. Proficiency in Linux, log analysis, malware detection & vulnerability detection, and cyber threats. Efficient in data analytics, reporting, and analyzing big data sets for potential anomalies. Successfully completed a Certified Information Security Professional (CISSP) boot camp. Technical Proficiency: Incident response, log, security incident management (SIEM), malware, and exploit analysis. Penetration Testing, threat modeling, social engineering, and testing methodologies (OWASP Top 10). Vulnerability management, vulnerability identification, classification, monitoring, and risk analysis, Operating systems, Linux, Windows, and Redhat. Networking, TCP/IP, wireless technologies, routers, switches, firewalls, and network segmentation. Technologies, Archsight, Spunk, Kali Linux, Bluecoat, Fireye, Wireshark, Metasploit, John-the-ripper, nmap, Python, Java, CSS, SQL, and HTML. Authorized to work in the US for any employer Work Experience Enterprise Vulnerability Management- Sr. Security Analyst Thomson Reuters August 2018 to Present Established remediation process and procedures drive critical vulnerabilities by safeguarding information systems connected to the corporate network. Stretched expertise by wearing multiple different hats- including windows engineer, vulnerability management, and remediation specialist to test, implement, and support patching to critical systems. Remediated critical risks affecting GDPR and provided subject matter expertise to keep servers in compliance before audit deadline. Crafted custom patch processes and frameworks to mature the vulnerability management team. Threat and Vulnerability Management - IT Security Analyst Express Scripts 2016 to Present Executed and coordinated vulnerability management efforts, based on industry standards, best practices, and established polices. Effectively communicated emerging critical vulnerabilities and patch strategy to client stakeholders including technical staff and leadership. Analyzed and assessed vulnerabilities in infrastructure (software, hardware, and networks) calculating risk to organization. Technical resource ensuring teams

remediate vulnerabilities within their service leasing agreement. Actively researched emerging threats, security trends, methodologies, technologies, and regulatory requirements. Responsible for PCI DSS assessments to ensure corporate meets regulatory compliance. Created and enhanced CIS benchmark hardening baselines within the organization. Computer Security Incident Response Team IT Security Analyst, Consultant Best Buy July 2015 to July 2016 Performed analysis of log files from variety of sources (e.g. individual host logs, network traffic, antivirus, firewall, and proxy logs) to identify possible infections. Monitored SIEM logging environments for security events and alerts to potential active threats, intrusions, and escalated accordingly. Performed assessment of network traffic leveraging Fireeye and network package captures identifying indicators of compromise (IOCs). Proactively documented malware analysis and wrote comprehensive auditable cases. Responsible for monitoring security tools and logs to identify based on enterprise acceptable use violations. Performed assessments on malicious phishing emails submitted to CSIRT. Trained new CSIRT analysts on incident response processes and platform usage. United Support Analyst, Consultant UnitedHealth Group February 2015 to July 2015 Identified and authorized access to subjects within the organization complying with confidentiality of PHI, PII, and HIPPA information. Adhere to corporate security policy providing guidance and technical awareness to stakeholders. Professionally provided top tier support for high volume call environment to over 4,800 corporate health systems, applications, VPN, VOIP, remote clients, and Cisco devices. Effectively translate complex concepts into easy English that non-technical oriented customers can understand. Technical Assistant Consolidated Communication January 2014 to January 2015 Managed a DHCP server suspending and authorizing network connected devices for residential and business customers. Implemented support for peripheral network connected devices, including routers, modems, IPTV, wireless access points, and peripheral equipment in a timely manner. Cleared out server sessions along with maintaining fifteen different email systems. Provisioned new customer s accounts and network equipment authorizing their access. Adhere to DMCA notices according to policy suspending customers violating DMCA regulations. Desktop Support Intern MEI-Total Elevator Solutions July 2012 to August 2013 Effectively investigated and

diagnosed malware on internal systems with Symantec Endpoint and performed reimaging, migration procedures to eradicate malware infections. Provided internal support for peripheral network connected devices, including patch management, system monitoring, and upgrading corporate systems. Responsible for upgrading all corporate systems to Windows XP to Windows 7. IT Help Desk Analyst Minnesota State University Mankato October 2011 to July 2012 Technical support resource for applications, operating system, and college software issues. Provided support for faculty grading systems and troubleshooted campus software over phone, internet chat, and email in timely manner. Education Bachelor of Science in Information Technology Minnesota State University May 2014 Associates Minnesota West Community College May 2014 Skills PAYMENT CARD INDUSTRY (2 years), PCI (2 years), REGULATORY COMPLIANCE (2 years), WIRELESS (1 year), Cyber Security, Cissp, Information Security, It Security, Qualys (2 years), Nexpose (2 years), Arcsight (1 year), Incident Response (2 years), Pentration Testing (1 year), Vulnerability Management (2 years), Redhat (2 years), Malware (2 years), Social Engineering (2 years), SIEM (2 years), Windows (6 years), FireEye (2 years), Firewalls (2 years), Wireshark (2 years), Cyber Defense (2 years), Security Analyst (5 years), Security Engineer (3 years) Links http://www.linkedin.com/in/garrett-nelson-ba301b54 Certifications/Licenses CompTIA Security+ May 2015 to May 2020 Nexpose Advance Certificated Administrator (NACA) September 2017 to Present

Name: Kimberly Bernard

Email: mckeedouglas@example.org

Phone: 252.643.6028