

Acting Sr. Director - Global Cyber Security Operations Center Acting Sr. Director - Global Cyber Security Operations Center Acting Sr. Director - Global Cyber Security Operations Center - Capital One Financial Charles Town, WV Work Experience Acting Sr. Director - Global Cyber Security Operations Center Capital One Financial - McLean, VA September 2017 to Present McLean, VA 09/2017 - Present Capital One Financial Corporation is a bank holding company specializing in credit cards, auto loans, banking and savings products. Acting Sr. Director - Global Cyber Security Operations Center ? Lead the Global CSOC, which includes four tiers of technical teams and the Incident Response and Incident Management functions for the enterprise ? Managed and led a team of 35+ associates with a budget of \$150k+. ? Regularly comply with internal and external regulator regarding our work as the 24x7 defense team of COF. ? Act as the Cyber Operations Sr. Director in their absence. ? Strategically set the groundwork for defensive operations automation and machine learning to streamline response and containment. ? Regularly provide program updates and metrics to Senior Leadership (CISO) and meet with them on a regular basis to address questions from the board of directors. ? Create and conduct training for all levels of the Fusion Center, to include Cloud security & investigations. Senior Manager - Global Cyber Security Operations Center ? Member and lead contributor of CSOC Leadership Team. ? Directly manage 10+ associates and lead CSOC operations during the day shift. ? Responsible for performance management, coaching, and associate mentoring. ? Build interorganizational relationships to strengthen the CSOC's capabilities and response time. ? Set and follow through on organization strategy and goals throughout the year. ? Develop and refine new hire on-boarding training as well as technical topic training within the organization. ? Develop and drive requirements for homegrown software solutions to be used in the CSOC, ultimately leading the onboarding and adoption of new technology. ? POC for all CSOC related matters at Capital One headquarters in McLean. Adjunct Professor - Cyber Security Blue Ridge Technical & Community College - Martinsburg, WV August 2016 to Present Martinsburg, WV 08/2016 - Present An HLC North Central Association of Colleges & Schools accredited technical and community college offering coursework in Business, Information Technology, & Cyber Security among other disciplines. Adjunct Professor - Cyber Security ?

Develop course curriculum. ? Teach CYBR-220, Wireless Security. ? Teach IT-105, Computer Ethics. ? Serve on the College Technical Advisory board providing recommendations, guidance, and subject matter expertise for implementations for new degree programs and technology solutions. Cyber Threat Intelligence - Senior Technical Specialist Inova Health - Sterling, VA October 2016 to September 2017 Sterling, VA 10/2016 - 09/2017 Inova is a not-for-profit healthcare system based in Northern Virginia that serves more than two million people each year from throughout the Washington, DC, metro area and beyond. Information Security Cyber Threat Intelligence - Senior Technical Specialist ? Build out the company's Cyber Threat Intelligence capabilities, as well as cyber incident response. ? Project management across applicable areas of Information Technology and Information Security. ? Build out and perform network and endpoint forensics. ? Monitor and administer network security stack to include SIEM, Malware Analysis, Content Analysis, IPS, & other perimeter defense tools. ? Implement and maintain evidence based research and technical practice for assigned EHR and system applications. ? Manage and maintain cyber threat intelligence platform and feeds. ? Cyber threat hunting and remediation. ? Vulnerability management and analysis. Senior Information Security Analyst Clarabridge, Inc - Reston, VA June 2013 to October 2016 Reston, VA 6/2013 - 10/2016 Privately held company providing customer experience management and engaging platforms, collecting and transforming customer feedback into intelligence, allowing businesses to activate the voice of the customer across the enterprise. Senior Information Security Analyst: Recruited as technical support analyst, shifting to information security to expand security program auditing, customer penetration testing, risk assessments, security countermeasure deployment, and vulnerability management. ? Set audit schedule, authoring audits to test against all security policies and collaborate to close gap findings. Contribute and lead SIEM enhancement by evaluating cyber threat trends. Administer resources (Windows, UNIX, Kali Linux and OSX/iOS) to test, evaluate, implement, and maintain security products (antivirus and SIEM). Spearheaded project for central antivirus management solution implementation; completing in time and in budget, resulting in saving \$45K annually. ? Lead SOC (security operations center) analysis, monitoring health and integrity of critical infrastructure, as well

as responding to security events, demonstrating appropriate remediation decisions and leadership escalation. Member of company CSIRT (Computer Security Incident Response Team) - clarifying analysis and report findings. Provide security awareness training (new hire, physical security, and HIPAA) and author / influence monthly security newsletters, increasing corporate event notification by 75% and reducing employee incidents by 50%. ? Evaluate and influence selecting and deploying security products, IT-related solutions, and approval process for changes within infrastructure and systems. Perform network vulnerability scans, SaaS penetration testing, evaluate results and steer remediation. Authored corporate Emergency Preparedness Procedures, and contributed to the development of internal assessment / pen testing (corporate, SaaS, and customer), reducing customer time-to-test from 60 days to two weeks. ? Identify distributed systems security issues and collaborate with business units and customers, ensuring mitigation in a timely manner. Welcome responsibilities, provide excellent client communication, and collaborate cross-functionally with consultants to resolve client issues. Influenced architecture redesign project and identified appropriate resources, enhancing security and availability of SaaS infrastructure, saving \$100K annually. Technical Support Analyst DataQuick Information Systems - Wilmington, DE February 2013 to June 2013 Wilmington, Delaware 2/2013 - 6/2013 Supplier of real estate data, analytics and business solutions to mortgage originators and servicers, investors, real estate professionals and public sector. CoreLogic acquired DataQuick in 2013. Technical Support Analyst: Provide Tier I/II support to internal customers and act as technical liaison between engineering and other business groups. ? Influenced web-based application support, analyzed issues, and documented remediation using C, Perl, C+, Java, .Asp, and PowerBuilder. Tapped to serve as technical liaison between internal departments, corporate departments, and vendors / customers, communicate customer needs to business units and technical representatives resulting in. ? Contributed and implemented new procedures and standards in support of department, division, and company goals. Performed system analysis, developed business requirements, and designed documents for existing and proposed systems. ? Audited and network gateway logs for anomalies and authored actions and remediation reports. IT Quality Assurance Specialist Penske Truck Leasing - Reading,

PA June 2011 to February 2013 Reading, Pennsylvania 6/2011 - 2/2013 Penske Corporation's Truck Rental company operating diverse truck rental fleet in North America ensuring customers enjoy high quality vehicles, service and peace of mind when renting trucks commercially or for a do-it-yourself household move. IT Quality Assurance Specialist: Facilitate and monitor compliance to the software development and testing methodologies. ? Facilitated and monitored the software development testing and compliance. Developed and executed software test plans, to include pre- and post- deployment to production. Led bi-weekly change control meetings to discuss and approve changes to mission-critical software ensuring project deliverables were on time and within budget. ? Influenced architecture and web development teams, ensuring web integrity of and security of backend infrastructure based on security review / analysis. Audited all software implementations, tracked defects, and authored reports geared for senior leadership and business units. ? Led support for mission-critical project management, software, and other internal applications used internationally. Contributed and influenced project that merged employee time management for both onsite and remote workers around the globe resulting in an increase in reliability and functionality of employee/contractor time tracking. Education Master of Science in Information Assurance and Security Capella University - Minneapolis, MN 2014 Bachelor of Science in International Crime & Terrorism Delaware Valley University - Doylestown, PA 2007 Skills Security, Dlp, Ids, Ips, Iso, Metasploit, Nessus, Nexpose, Nist, Nmap, Snort, Splunk, Wireshark, Tcp/ip, Firewall, Malware, Linux, Unix, Unix shell, Wireless Links <http://www.linkedin.com/in/jamesyarnall> Additional Information Areas of expertise include: * Audit / Security * Vulnerability * Linux/Windows Skills & Abilities Standards: NIST (800-53 and 800-88), ISO (27002), OWASP Operating System: Windows, Linux, Mac OS X, Kali Network: Ethernet, T1/T3, Wireless, TCP/IP, UDP Security: Firewall (pfsense, FireMon, Checkpoint), IDS/IPS (SourceFire, Snort), Metasploit Pro, DLP, HIPS, System Hardening, Antivirus (Symantec, Sophos, Cylance), Penetration Testing, Incident Handling, Nmap, Nessus, Wireshark, Burp Suite, SecureVue, Advanced IP Scanner, OWASP ZAP, Fiddler, Metasploit, Nexpose, Splunk, & BlueCoat content/malware analysis. Languages: (High Level) UNIX shell, Python, Ruby, Java, HTML Applications: Microsoft Office, GSuite

Name: Karen Kim

Email: becky71@example.net

Phone: 550-682-4668