Senior IT Security Analyst Senior IT Security Analyst Streamwood, IL Authorized to work in the US for any employer Work Experience Senior IT Security Analyst October 2016 to Present Information security monitoring of the client's enterprise network, incident response, malware analysis, root cause analysis, development of the information incident response processes and practices, vulnerability scanning, event log analysis including firewall and proxy traffic, proxy server management, tuning and creating policies/rules for security appliances. OpenDNS, CrowdStrike - Falcon, Qualys, CyberArk - ViewFinity, ServiceNow Ticketing & Incident Response Primary contact and lead for SecOps and IR related incidents and/or issues. Trained and mentored Jr Security Analysts Achievements: Created official incident response policies and procedures Created and documented policy and procedures in regards to vulnerability management, various type of alerts analysis and suspicious email analysis. Successfully deployed and managed Cisco OpenDNS and CyberArk ViewFinity products for client and its 28 Operating Companies. Built SOC and trained Security Ops and Incident Response team members. Created SOC-wiki. IT Security Analyst Arthur J Gallagher - Itasca, IL November 2014 to October 2016 Information security monitoring of the Arthur J Gallagher global enterprise network, incident response, malware analysis, root cause analysis, development of the information incident response processes and practices, vulnerability scanning, event log analysis including firewall and proxy traffic, proxy server management, coordinated tuning of security appliances with the security engineering team and patching with system operations team. McAfee ePO, IBM QRadar, Solarwinds, SourceFire, FireEye, TripWire IP360 Vulnerability Scanning, Administering Tripwire IP360 Suite, Application Scanning, Symantec MessageLabs, Remedy Ticketing & Incident Response, Process Development & Security Incident Life Cycle Management- M&A Security Compliance Process Development Achievements: Created official incident response policies and procedures that SOC team currently follows. Created and documented policy and procedures in regards to vulnerability assessments for new businesses and worked closely with upper managements such as IT Directors, project managers, executives and various teams in order to satisfy the security requirements and also the business needs. Drove security vulnerability assessment project scanning and remediation for

about 20 business acquisitions. Guided technicians in remediation efforts and coordinated with IT Directors, project managers and other teams to drive completion in correlation to business needs as well as driving development of information security compliance standards for mergers and acquisitions through vulnerability scanning and assessments. Teamed up with the security engineer in order to successfully and in timely manner finish the migration of the new IP360 appliance (VnE). Provided SIH and QRadar training to the higher management (i.e. executives, IT directors), members of the various teams (i.e. UK System Operations and Security) and new team members of the SOC team. United Technologies (Contractor through Kelly Services), East Hartford, CT IT Security Monitoring Analyst/SOC Analyst 2012 to 2014 Identify viruses, document and submit to Symantec for proper handling. Recognize and properly handle IPS attacks, known bad destinations, large data transfers, and suspicious internet traffic. Analyze and properly handle SPAM email. Monitor network and communications traffic from multiple sources to identify unauthorized or suspicious activity. Identify anomalies and determine root cause and potentially malicious data. Report security incidents to appropriate departments. Qradar, Fidelis XPS, FTK Imager, Forensic Toolkit, PRTK Education BS Utica College Information Systems Management Rasmussen College Skills SECURITY (5 years), DATA INTEGRITY (Less than 1 year), EXCELLENT COMMUNICATION SKILLS (Less than 1 year), PROBLEM SOLVER (Less than 1 year), SYSTEMS SECURITY (Less than 1 year) Additional Information AREAS OF EXPERTISE Network and Systems Security ? Data Integrity ? Impact Analysis ? Web Security ? Digital Transmission Analysis ? Analytical Problem Solver ? Attention to Detail ? Excellent Communication Skills

Name: Cassandra Kelly

Email: frederick03@example.net

Phone: 9806291706