Full Time Employee Full Time Employee Full Time Employee - Marathon Oil Houston, TX Multi-faceted experience with IT Security of organizations; particular strengths include: Developing and implementing innovative IT Security programs and products and services. Leading and Optimizing the Cybersecurity through periods of downturn and transition. HARDWARE & SOFTWARE EXPEREINCE Software & Hardware Windows 10, Windows 7, Windows 2008 R2, Windows 2012, 2016 server Microsoft Office 2016, 2013, 2010, 2007, LAN Guard, Wireshark, Nessus, Retina, Nexpose, Remedy, Peregrine, Altiris, Service Now SIEM Splunk, Nitro, Q-Radar, Arc-site ProofPoint, Barracuda SAP Security & Activate Directory Security FireEye, Palo Alto Firewall Carbon Black - Bit 9 Palo Alto Traps, Cisco AMP Websense, Blue Coat, Zscaler, Forcepoint TCP/IP, IPSEC, DNS, DHCP, Cisco VPN, Global Protect Symantec & McAfee, Trend Micro, GFI Viper, Sophos, System Center Enpoint Protection Compliance Standards SOX/NIST/SCADA/DCS Authorized to work in the US for any employer Work Experience Full Time Employee Marathon Oil - Houston, TX September 2015 to Present Cyber Threat Intelligence Analyst In-depth knowledge of architecture, engineering, and operations of enterprise SIEM. Ingested log sources for Security operations and Threat Analysis team. Deployment of vulnerability scanner agents and management consoles based on compliance requirements. Conducted vulnerability scans for every region within Marathon. Executed Penetration tests and provide remediation actions for various IT groups and products Demonstrated experience with handling incident response and able to communicate and coordinate when incidents occurred. Experience with threat and malware analysis as well as working with third party forensics tools for incident handling. Provide actionable cyber threat intelligent information for executive management relative to the business Worked on the Implementation of DLP polices and classification with legal. Architecture, engineering, and administration of enterprise Privilege Access Manager (PAM) Threat Monitoring Analyst Lockheed Martin - Houston, TX May 2015 to August 2015 Incident handling experience and advanced understanding of networking, system -Unix/Linux command line experience In-depth knowledge of operations of enterprise SIEM platforms (QRadar, Splunk) Demonstrated experience with Computer Incident Response

Experience and proficiency with Anti-Virus, HIPS, ID/PS, Full Packet Capture, Host-based Forensics Experience with malware analysis concepts and methods. IT Security Operations Manager, North & South America Regions Foster and Wheeler/AMEC (FTE) - Houston, TX August 2012 to May 2015 Responsible for the activities of IT security (SIEM, incident response, DLP, Security auditing and compliance) Audit based on SOX, HIPAA, compliance and worked with legal and finance to ensure auditing governance was followed. Conducted investigations based on requirements from Legal and HR. Maintaining IT security for Foster Wheeler Americas for over 3200 users in various countries. Created Cyber security IT security policies and practices. Responsible for identity management access (IAM) for all the Americas offices. Application Security testing for new and existing commercial applications as well as company developed applications. Responsible for the activities within the IT security department as penetration testing, vulnerability scanning and remediation testing. Plan and prepare for future improvements to various types and operating levels of IT security hardware and software. Recommend IT security solutions within budget Information Assurance Security Officer KBR - Houston, TX May 2009 to August 2012 Providing patch management to systems using WSUS and GFI LanGuard, also developing Information Assurance regulations. Managing web content filtering and routers and switches. Conducted vulnerability assessment using various scanning software including Retina. Deployment of Vista Enterprise with MDT and GPO management. Managed centralized Symantec Endpoint anti-virus servers. Performed security audits on network and provided user awareness training. Develop policies and guidelines within the organization. Tested commercial software for security and compatibility and compliance. Information Assurance Security Officer DRS Technical Services Inc July 2007 to May 2009 Implemented patch management system WSUS for over 5000 customers. Managed web content filtering. Conducted vulnerability assessment using various scanning software including the following (ISS, Harris Stat, and Retina). Managed centralized anti-virus server for over 5000 customers. Preformed audits on networks for the Iraq Theater of Operations Provided user awareness training users. Ensured compliance per DOD regulations. Maintained and troubleshoot user accounts and policies within Active Directory and Exchange. Tested

commercial and Government software for security and compatibility and compliance. Maintained and secured network infrastructure for Department of Defense. Modify Checkpoint Firewalls as needed to meet IT Security standards Desktop Support Analyst Sr Halliburton Company - Houston, TX April 1998 to June 2007 Desktop Analyst Citation Oil & Gas Corporation - Houston, TX December 1996 to December 1997 United States Marines August 1992 to December 1996 Education Bachelor of Science in Information Technology in Information Technology Capella University - Houston, TX May 2020 Skills Cyber Security (8 years), Desktop Support (10+ years), IT Management (2 years), Active Directory, Security Military Service Branch: United States Marines Service Country: United States Rank: Corporal August 1992 to August 1996 Certifications/Licenses CompTIA Security+ April 2010 to Present

Name: Natalie Gibson

Email: mcdowelljoseph@example.net

Phone: 9446202419