Senior Data Security Engineer Senior Data Security Engineer Senior Data Security Engineer - WEXNER MEDICAL CENTER AT Reynoldsburg, OH To obtain a challenging position within an environment focused on PC support, networking and cyber security that allows for growth and advancement. MAJOR QUALIFICATIONS Network Hardware/Software: Network Hardware/Software: Novell, IE 6.0 - 11, Office XP -2007, McAfee EPO, EMM, Symantec A\V (SEP), Symantec DLP, IBM Site Protector (SIEM), LogLogic, Wireshark, Winpcap, Webmarshal Proxy, Fireeye, Secureworks IDS Monitoring, Retina CS, Nessus, IronPort Proxy, Graylog, Netspective (webFilter), Proofpoint (Mail Filter) Service-now, GOOD, DDPE, Altiris, Proofpoint, QRadar, and Splunk Authorized to work in the US for any employer Work Experience Senior Data Security Engineer WEXNER MEDICAL CENTER AT May 2012 to Present The Data Security team is responsible for planning, engineering, development, implementation and compliance monitoring for organization wide security programs. Maintaining and ensuring the protection of HIPAA regulated information PHI, PCI, PII, utilizing Altiris, DLP, Firewall, email monitoring (Proofpoint), proxy (Iron Port), virus (McAfee ePO, Forefront), web filtering (Netspective), encryption (Truecrypt, McAfee EERM, EEPC, BitLocker, Ironkey, Safeboot), MDM solution for BYOD (McAfee) and vulnerability scanning tools (Nessus, Accunetix) to gather the necessary intelligence for investigation in order to develop security policies and standards based on HIPAA requirements. Utilize ServiceNow to create tickets when further remediation is required. Help to develop security policies and standards, performed risk assessments, helped to approve firewall rule request, attend Architect s meetings and oversee various projects as assigned. Also primarily responsible for the vulnerability management platform and process which encompasses Tenable Nessus scans, processes and associated reporting. Lead vulnerability remediation and follow-up efforts as well as provide status to upper management as well as presentations related to vulnerability remediation projects. Cyber Security Analyst AMERICAN ELECTRIC POWER August 2009 to May 2012 The SOC is responsible for maintaining and ensuring a strong security posture through the continuous monitoring, expert analysis of data, and immediate response to potential security threats. This includes gathering, investigating, and analyzing security related events from multiple sources to

include firewall, intrusion detection, host intrusion prevention, and others. Gather intelligence about security related threats and disseminate information as appropriate. Optimizing current security related products to increase response time and effectiveness. Investigate a security alert and provide either a resolution or escalate a detailed analysis to senior security staff. Security applications used are Proof Point, Log Logic, EPO3, 8E6, SiteProtector, QIP, Webmarshall Proxy, Fireeye, SIEM, Wireshark, Sentinel and McAfee. Followed NERC-CIP Standards. PII, ITIL training and implementation as required. IT Support Specialist II AMERICAN ELECTRIC POWER September 2008 to September 2009 Perform a wide variety of specialized telecommunications system with 24/7 monitoring, testing and troubleshooting functions dealing with network management and network surveillance of digital/analog microwave systems, alarm systems, optical transmission and various multiplexing equipment. Apply new technologies and systems as needed to provide adequate customer support to internal and external telecommunications customers, coordinate system outages. Monitoring LAN/WAN, SCADA RTU, MDC and radio devices throughout AEP's system. Tools used are HPOV, Harris, Fault Management System, Remedy, Pingmon, SDG Explorer, Token 2, Preside, Call Monitor, NetQoS and Telnet. Coordinate site/facilities access. FAA NOTAM's, OUPS and Texas One facilities locate requests. Coordinate network schedule maintenance Outage request, Outage pre-approvals, Outage notifications with internal and external customers. Troubleshoot telephone trouble and Voicemail password resets, SCADA Sub stations RTU outages, Desktop Application trouble, Mobile Data and Audio Radio trouble, LAN and Server outages. Create and modify user profiles in the OCTEL and Cisco Call Manager phone system. Provide support and work with IT Command Center- Security, Physical Security, and IT personnel in all aspects of the network for AEP. IT Support Specialist II AMERICAN ELECTRIC POWER June 2004 to September 2008 Level 1 & 2 application\hardware support: Supported Windows XP and 2k operating systems. Supported Fiberlink (used to connect to the corporate VPN via dial-up, broadband, wireless connections). Supported Office applications, Lotus Notes several web based applications. Utilized the LANDesk remote control tool, MS NetMeeting, Active directory, Ace, oracle password tool, security information system, Peoplesoft password reset\Time entry, mainframe

support, Remedy support tool, AEP Cellular and paging calls, VOIP phone issues, Blackberry, various other handheld devices. Business Analyst II American Electric Power (DWMS WORK MANAGEMENT) September 2003 to June 2004 Level 2 application support: Supported proprietary applications ie: (Landesk) Iowa, Spectrum, MACSS, Storms and Fieldview in a WIN 2K environment. Used the Remedy trouble ticketing system. Supported MDC (mobile data computers). Used various web tools for troubleshooting. IT Support Consultant(Helpdesk) TEK SYSTEMS June 2003 to August 2003 IT Support Consultant (Help Desk) SOPHISTICATED SYSTEMS, INC - Columbus, OH November 2000 to September 2002 Help Desk Consultant Education Associate of Applied Science degree in Applied Science FORTIS COLLEGE June 1994 Technical Management DeVry INSTITUTE OF TECHNOLOGY Skills Linux (Less than 1 year) Additional Information Operating Systems: Windows 3.1x, - 7, Linux

Name: Debra Wright

Email: jfischer@example.com

Phone: 477.560.5664x221