Consulting Systems Engineer I (SOC Lead) Consulting Systems Engineer I (SOC Lead) Consulting Systems Engineer I (SOC Lead) - BNSF Railway Cyber security professional whose qualifications include a Master's of Science in Information Systems, GXPN, GCFA, SSCP and Security+ certifications. Experienced in threat and vulnerability analysis, security event monitoring, SOC process development, incident response and security systems administration. Authorized to work in the US for any employer Work Experience Consulting Systems Engineer I (SOC Lead) BNSF Railway May 2014 to Present SOC Lead Support Tier 1 threat identification and analysis Perform Tier 2 incident validation and escalation Architect SOC security monitoring Develop security monitoring dashboards, panels, and reports. Develop processes and procedure Perform digital forensics and some reverse engineering SOC systems administration (Splunk) Provide daily support and training for team members. SOC Engineer BNSF Railway March 2014 to June 2014 - contract-to-hire) Daily threat event monitoring, identification, analysis and escalation Identify vulnerabilities and work with appropriate teams for remediation. Perform security systems administration (e.g., FIM, SIEM, AV) Process development Developed Splunk dashboards, panels and reports. Cyber Security Analyst Energy Future Holdings November 2013 to March 2014 - contract-to-hire, recruited by previous manager) Performed daily threat and vulnerability analysis Vulnerability scanning and reporting Security systems administration(e.g., SIEM, AV) Process development Interviewed potential SOC analysts Trained new-hires Security Engineer Matrix Resources (Pioneer Natural Resources April 2013 to November 2013 - contract-to-hire) Threat and vulnerability analysis Security systems upgrades (AV) and administration (AV, Proxy, Firewall) Penetration testing for vulnerability validation Vulnerability assessment Process development Firewall policy review IT Security Analyst Pier 1 Imports December 2011 to March 2013 Threat and vulnerability assessment Vulnerability scanning and reporting Security monitoring Security systems installation, upgrades, and administration (SIEM, FIM, AV, IPS, Firewall, Scanner) Firewall policy review Participated on the Pier 1 Architecture Committee Product assessments POS Support Tech I/II Radiant Systems January 2009 to December 2011 Acquired by NCR) POS software support for NCR channel partners Supported clients with PCI compliant systems configuration Software bug detection and documentation Network, OS and NCR applications troubleshooting Biometrics configuration and troubleshooting Technical Support (Contract) Technical Focus (GameStop Contract) June 2008 to December 2008 Router configuration Router installation support SAP Jr. Basis (Contract) Komava SAP Providers LLC - Grapevine, TX December 2007 to June 2008 System monitoring and troubleshooting Netweaver 2004s installation Content server installation TREX search engine troubleshooting Certifications/Licenses GCFA GXPN Additional Information Core Competencies SOC Team Building Threat & Vulnerability Analysis Incident Response SOC Process Development Security Systems Administration Digital Forensics (Disk/Memory) Security Monitoring Operating Systems: Windows Server 2003-2008, Win95-8, RedHat, AIX, Ubuntu, Debian Databases: SQLServer, MySQL, Oracle SIEMs: Splunk, LogLogic, McAfee ESM Vulnerability Scanners: Nexpose, Qualys, and Nessus Pentesting Tools: Python, Nmap, Netcat, Tcpdump, Scapy, Burpsuite, Metasploit, Kali Linux Firewalls: Palo Alto and Cisco ASA Proxies: Websense and Bluecoat Intrusion Prevention Systems: HP TippingPoint, Palo Alto, and a proprietary applications Debuggers/Disassemblers: WinDbg, Immunity Debugger, OllyDbg, IDA Access Controls: RSA, Entrust and Safenet, Active Directory Antivirus: McAfee, Sophos, Symantec File Integrity Monitor: Tripwire, EasyFIM, OSSEC Languages: Python (Proficient), HTML (intermediate), PHP (intermediate), JavaScript (intermediate), SQL (intermediate), Assembly (basic), C (basic), PowerShell (basic), Bash (basic), VBScript (basic), Ruby (basic) Forensics Tools: TSK, Volatility, Bulk_Extractor, Foremost, Log2timeline, SIFT Workstation

Name: Kenneth Mosley

Email: uelliott@example.com

Phone: 891.473.7434x67020