Head IT Security Analyst Head IT Security Analyst Head IT Security Analyst - EagleForce Associates Gaithersburg, MD Work Experience Head IT Security Analyst EagleForce Associates - Herndon, VA November 2016 to Present Monitoring   Monitor the security of critical systems (e.g., e-mail servers, database servers, web servers, etc.) and changes to highly sensitive computer security controls to ensure appropriate system administrative actions, investigate and report on noted irregularities.   Conduct network vulnerability assessments using tools to evaluate attack vectors, identify system vulnerabilities and develop remediation plans and security procedures.   Ensure organizational compliance with CFCU information security programs.   Manage the SIEM infrastructure using SPLUNK technology.   Conduct routine social engineering tests and clean-desk audits.   Investigate potential or actual security violations or incidents in an effort to identify issues and areas that require new security measures or policy changes.   Strategy Development   Research new developments in IT security in order to recommend, develop and implement new security policies, standards, procedures and operating doctrines across a major global enterprise.   Define, establish and manage security risk metrics and track effectiveness.   Coordinate with third parties to perform vulnerability tests and create security authorization agreements and standards.   The ability to balance risk mitigation with business needs.   Disaster Recovery   Collaborate with business units to determine continuity requirements.   Conduct business impact analysis for vital functions; document recovery priorities of the key processes, applications and data.   Establish disaster recovery testing methodology.   Excellent decision-making abilities that help analyze a situation and provide feasible solutions promptly Competent in technical aspects of disaster recovery analysis   Identify the low performing areas of the organization and conduct a root cause analysis of the same   Plan and coordinate the testing of recovery support and business resumption procedures while ensuring the recovery and restoration of key IT resources and data and the resumption of critical systems within the desired timeframe. Penetration testing   Performed risk assessments to ensure corporate compliance   Developed agenda for quarterly audit program   Conducted security event monitoring for corporate wide in-scope applications   Performed application security and penetration testing using Metasploit

Framework   Leverage custom exploits   CCNA   Managed installation, configuration and administration of Cisco equipment in IT architecture of organization.   Configured IT LAN/WAN elements and held responsibility of maintaining and monitoring performance of network.   Provided Tier1 technical support; assisted users facing network problems. Performed advanced troubleshooting, diagnostics and provided tier/level-1 solutions to network failures.   Excellent troubleshooting skills, be able to triage a customer's issue, getting to the root of the problem, document issue in Help Desk application.   Help Desk Analyst   Handle technical troubleshooting within an enterprise environment, including system crashes, slow-downs and data recoveries. Engage and track Priority 1 issues, with responsibility for the timely documentation, resolution and closure of trouble tickets.   Diagnose, troubleshoot and resolve a range of software, hardware and connectivity issues. Excel in asking probing questions and researching, analyzing and rectifying problems.   Documented all inquiry activities in the appropriate reporting system. Education Masters in Cloud computing architecture UMUC University of Maryland University College (UMUC) December 2019 Bachelor of Science in Computer Networks and Cyber Security in Cyber Security University of Maryland-University College - Adelphi, MD Skills audit (2 years), database (2 years), Disaster Recovery (2 years), Security (2 years), solutions (2 years), Cyber Security, It Security, Information Security Certifications/Licenses Security+ September 2015 to September 2021 Certified Ethical Hacker (CEH) February 2017 to February 2020 CCNA Routing and Switching Additional Information TECHNICAL SKILLS: Software: Wireshark, Snort, Nmap, Nessus   Hardware: Servers, switches, routers, computers, cell phones, printers   Operating systems: Linux| Windows | Mac OS X Skill Highlights   Information risk management| Security controls| Regulatory compliance   Technical audit| Project management| Leadership |communication skills Key Skills: Excellent decision-making abilities that help analyze a situation and provide feasible solutions promptly   Competent in technical aspects of disaster recovery analysis   Ability to communicate effectively and efficiently   Highly skilled at managing multiple tasks simultaneously   Brilliant logic building and problem solving skills Technology Skills   Security: Advanced user of intrusion-detection, IDS/IPS (Snort), DLP, vulnerability-scanning, and antivirus tools   Systems: Experience working in

mixed Windows/Linux, database and virtualized/physical server environments   Programming: Some knowledge of basic Bash scripting, Html

Name: Peter Clark

Email: zachary72@example.com

Phone: (207)835-7645x237