IT Security Analyst IT Security Analyst IT Security Analyst - THANOS CONSULTING Frisco, TX I have proven track record of 10years in designing, preventing, detecting various form of attacks on computer infrastructure and software to reduce potential data compromise. Ability to work in a fast-paced environment, Multi-Tasker, Easily adaptable to working within team. Microsoft Office experience and Knowledge of Ticketing systems, Fundamental knowledge and understanding of TCP/IP, routing and switching. Hands-on experience using tcpdump. Knowledge of or experience with SIEM technologies monitoring IDS/IPS alerts (Puppet, Salt, McAfee, LogRythem, ArcSight, Splunk, FireEye, Carbon Black) Work Experience IT Security Analyst THANOS CONSULTING - McKinney, TX July 2016 to Present   Carried out Risk Assessment / continuous monitoring to ensure threats are mitigated and appropriate controls are in place; coordinating with key partners in other IT and business groups to analyze threats and potential mitigations. Risk acceptance analysis and processing   Coordinating response to known vulnerabilities in IT infrastructure and applications. Conduct advanced computer and network forensic investigations relating to various forms of computer intrusion, theft of information, denial of service, data breaches   Monitoring for potentially malicious activity and responding to cyber security incident.   Testing for Change Management Controls ensuring only appropriately authorised, tested, and approved changes are made to applications, databases and OS. Also ensuring changes are tested before applying in production environment. Also ensuring no conflict of duties in the process.   Reviewing user policies, job functions, permissions and authorisation from time to time to ensure least privilege policy is enforced   Testing and Reviewing Backup and Recovery plan to ensure backup data is truly recoverable in event of an incident or disaster.   Assisted in Policy development and PCI-DSS Compliance, ensuring IT Governance objectives set by senior management are efficient and working as intended   Experienced carrying out Infrastructure testing in Windows, UNIX, and Mainframe environments. Assist with the development and testing of effective remediation plans for control deficiencies in addition to identifying areas for improvement, and discuss findings and recommendations with the process owners.   Identifying with Data owners/custodians to determine the appropriate classification of data and proper security controls. Assisted and identified with department heads to

update the IT Asset register.   Conducted phishing email assessments/ awareness tests to prepare and familiarize internal users with phishing attacks.   Working with the ISO and senior management to establish and define security baselines and metrics.   Conducted Security training and awareness to internal users via classroom presentations, posters and email from time to time.   Worked with the Technical teams to ensure security best practices are implemented at all levels.   Worked with third party application vendors/ clients to ensure appropriate security standard and compliance with regulations. Ensured all vendor patches are applied and up to date.   Knowledge of and maintaining awareness of emerging threats and their countermeasures. Anti- Cybercrime Superintendent AMERICA INTERNATIONAL INSURANCE COMPANY (NIGERIA) September 2011 to March 2016 Monitors and analyzes email alerts from a wide array of security devices and systems (SIEM's, Firewalls, IDS/IPS, WIPS, Systems, Networks, Anti-virus, etc.)   Creates Tickets internally and externally to track all activities.   Provide direct support to Clients via Phone, Email, SMS. Prepares and maintain the Administrative Documentation in a secure manner.   Update Management on any client changes.   Prepares Shift Activity Reports for clients and Management. Prepares Weekly and Quarterly summary reports for Clients and Management.   Maintain weekly communication with Clients, providing support and answering any questions or concerns in a timely manner to enhance S3's relationship as the Client's security partner.   Perform Quality Assurance by performing spelling and grammar check of final Reports. "Cleaning Up" all documents to look clean and professional; and are in the S3 approved template   Respond to customers in a positive and timely manner.   Respond to concerns, questions and issues by maintaining direct and continuous contact with Clients.   Security monitoring and analysis, cyber threat analysis, vulnerability analysis, or similar cyber security related field, incident management.   Responsible for conducting walkthrough interviews, updating and documenting process flow charts. Identified and tested IT Control and reported issues for further investigation and resolution.   Participated in integrated IMS audits- carrying out ITGC testing and assessment.   Reviewed documentation of clients' internal controls related to both IT and business cycles   Prepared plans for scheduled and unscheduled audits for PCI DSS compliance.   Responsible for auditing the company's technology

processes by identifying issues, developing test steps, reviewing and analyzing evidence. Assisted with the preparation of audit reports and presentation to business unit heads and management. Conducted vulnerability assessment testing, analyze results and presented the reports and findings to senior management. Monitor and reviewed System, Event, Access and Security logs from time to time. IT Consultant TIMELY TECHNOLOGY LTD May 2009 to August 2011 Administered and maintained all servers and network Managed User accounts and policies over the network Provided IT support to all staff as in-house Computer Consultant Assisted the company's staff in remote branches Carried out back up of the server from time to time Assisted in software projects for clients Worked with the global MIS team with headquarters in France Served as primary contact for telecommunication carriers and service providers and as well coordinated circuit design, provisioning, installation and troubleshooting Applied necessary updates and patches to all system from time to time Prepared a list of procedures to resolve most common tasks/problems experienced by users on site as reference for other members of staff Assisted in the update of Company's Asset Management System/ HR and Payroll system including providing after sales support of the software to clients. Delivered presentation on company bespoke software to prospective clients and as well provided training and upgrades to the existing ones. Also attended business meetings with clients. Carried out the setup and installation of computer systems Provided second level support to Clients and escalated problems to other departments/ Staff where necessary Carried out computer troubleshooting, repair, network installation and system Managed the company website ensuring data content is up to date Software installation, support and upgrades for employees and customers Responsible for equipment inventory management for several client Education Introduction to Cybersecurity for Business University of Colorado 2017 Harvard Business School - Boston, MA 2017 Masters in Personnel Psychology in Personnel Psychology University of Ibadan 2010 to 2012 Skills Security, Business continuity, Cobit, Disaster recovery, Dlp, Encase, Ids, Ips, Iso, Iso 27001, Nist, Nmap, Pci, Wireshark, Active directory, Network security, Configuration management, Mdm, Frameworks, Wireless Additional Information SKILLS/TOOLS - IT Risk Assessment, IT Control Auditing, Infrastructures, Vulnerability

Management (Testing/Assessment/Compliance), NIST800-37 - Securing Switches, Routers, Wireless Networks, Operating Systems and Passwords - Network Security, Cyber securities and threats, Asset Management, Due Diligence, Security Documentation/ Frameworks (ISO 27001, COBIT, PCI-DSS, NIST, ITAF), Patch Management, Configuration Management, (Active directory, Backup and Recovery), - Knowledge of tools like Nessuss Vulnerability Scanner, Wireshark, Ethereal, Netstat, Traceroute, Ping, IPS/IDS, MDM software, DLP software, Encase, Nmap; - Securing Operating System (Apple, Linus, Microsoft) Network switches, routers, wireless access point, signature analysis and physical security; - Business Continuity/Disaster Recovery Plan, Incident Prevention and Response documentation; OSX, SOC, Report writing and recommendations

PERSONAL SKILLS Ability to adjust to cultures and practice of organisation, work with and interact in a team. Good communication, self motivating and willingness to learn; and strong sense of leadership.

Name: Rachel Fields

Email: lisamiles@example.net

Phone: 363-629-4810x47333