IT Security/Incident Response Analyst IT Security/Incident Response Analyst IT Security/Incident Response Analyst - Keane Group Houston, TX High-performing, dedicated and enthusiastic individual with strong capabilities and motivation to achieving success in projects and organizational goals. Possesses good knowledge of IT Security Risk and Compliance, Enterprise Resource Planning (ERP), and IT Services Management (ITSM). Great team player and collaborator, with strong value addition and excellence. Work Experience IT Security/Incident Response Analyst Keane Group - Houston, TX February 2017 to Present Actively protected IT assets and infrastructure from external or internal threats and ensure that the company complies with statutory and regulatory requirements regarding information access, security and privacy Review firewall logs looking for malicious activity, threats, unusual traffic, indicators of attacks and indicators of compromise. Monitored and responded to alerts from Intrusion Prevention Systems (IPS) and Intrusion Detections Systems (IDS) Investigated incidents using Splunk. Analyze and correlate logs from various sources like webserver, proxy, firewalls and net-work and endpoint security products Triage and prioritize incidents and also work with the appropriate departments to undertake remedial actions. Perform incident root cause analysis and propose tailored and appropriate mitigation efforts Organize knowledge transfer sessions with junior analysts giving them the necessary and skills to be effective Malware analysis using Encase Forensics, Mandiant Redline and Volatility Investigate incidents from start to finish and produce detailed incident reports Responsible for deploying and managing bromium endpoint security Prepare weekly qualys scans and forward them to the qualys engineer to decimate to the various parties Assisted with the development of processes and procedures to improve incident response times, analysis of incidents, and overall SOC functions Provided network intrusion detection expertise to support timely and effective decision making of when to declare an event a security incident Documented all activities during an incident response and providing leadership with status updates during the life cycle of the incident Performed analysis of network and host-based security appliance logs (Firewalls, NIDS, HIDS, Sys Logs, etc.) to determine the correct remediation actions and escalation paths for each incident Provided information regarding intrusion events, security incidents, and other threat

indications and warning information Performed malware analysis through dynamic or static analysis Performed network and system analysis on how malware was introduced and propagated Worked with a variety of internal and external resources to understand latest security threat IT Audit/Compliance Analyst Halliburton - Houston, TX February 2015 to November 2016 Evaluated compliance with corporate security policies from planning phase to completion using COBIT, COSO, FISCAM, PCI DSS, SOX, SSAE 18 and HIPAA Frameworks in performing audit. Performed IT general controls testing for Sarbanes-Oxley (SOX) 404 compliance, and Service Organization Control (SOC) reports /SSAE18 (formerly SAS 70). Performed IT Infrastructure Audit to test default account, vendor update & patches, password setting and unnecessary services running over the application such as Unix, Window, Mainframe, Network devices, Firewall, Database and Active Directory. Participated in SAP Transaction testing to perform, including testing of segregation of duties to assist the client in improving their user management, authentication management, authorization management, access management, and provisioning capabilities. Tested General Computer Controls and Business Process Application controls using COSO, COBIT, PCI DSS and NIST 800- 53 rev. 4 frame works and performed walkthroughs and detailed testing of controls to evaluate the design and operating effectiveness of controls in federal government agencies. Performed walkthroughs and detailed testing of controls to evaluate the design and operating effectiveness of controls. Communicated IT audit findings to both senior management and clients Helped identify performance improvement opportunities for assigned clients Assisted in IT management in identifying gaps between policy and process, developing recommendations to remediate control weaknesses and be responsible for developing and maintaining IT control metrics related to compliance activities. Experience in IT auditing with emphasis on commercial public companies and federal government departments using ITGC and Application Controls. Ensure that policies and procedures are implement and processes are well documented and perform internal reviews, which identify compliance problems that call for formal attention. Coordinated with IT department and external auditors during SOX IT testing Evaluated the design and effectiveness of technology controls throughout the business cycle IT Security and Compliance

Analyst AOS-Orwell - Lagos, NG July 2011 to May 2014 Nigeria) Continuously updated the company's incident response and disaster recovery plans Document security breaches and assess the damage they cause Worked with security team to perform passive vulnerability tests to uncover system vulnerabilities. Fixed detected vulnerabilities and maintain a high- security standard. Monitored security access. Research security enhancement and make recommendations to management. Stayed up-to-date on information technology security trends and standards. Monitored computer networks for security issues. Installed security measures and operate software to protect systems and information infrastructure, including firewalls and data encryption programs Collect and manage technical intelligence from malware analysis to determine if its related to a campaign Collected and manage information from public and private sources for attribution and campaign correlation Identified and evaluate complex business and technology risks and security controls took multiple requirements (regulatory, technical, business) and integrate them into a framework Performed security risk analysis and gap assessments to identify opportunities for improvement Designed a strategy and detailed implementation roadmap Assisted in the selection and tailoring of approaches, methods and tools to support service offering Facilitated use of technology-based tools or methodologies to review, design and/or implement products and services IT Support Engineer Layer3 Limited - Lagos, NG February 2009 to June 2011 Nigeria) Planed, implemented and upgraded security measures and controls Protected digital files and information systems against unauthorized access, modification or destruction Maintained data and monitored security access Conducted internal and external security audits Managed network, intrusion detection and prevention systems Analyzed security breaches to determine their root cause Recommended and installed appropriate tools and countermeasures Defined, implemented and maintained corporate security policies Assisted with Security awareness training Coordinated security plans with outside vendors Improved process flows and problem resolution by tracking customer interactions and escalation. Provided on-site initial configuration and installation of access routers in a POP network. Troubleshoot and resolved LAN/WAN connectivity issues Provided help-desk technical support for installation, integration, and maintenance on the

Juniper Digital Broadband Delivery System Supported Juniper routers, switches, LAN to internal and external customers Education Associate of Applied Science in Petroleum Engineering Technology Houston Community College - Houston, TX May 2015 Bachelor of Science in Engineering Physics Federal University of Technology Akure December 2009 Skills SECURITY (6 years), INCIDENT RESPONSE (4 years), PCI (1 year), NIST (1 year), FIREWALL (3 years) Additional Information SKILLS Incident Response. Risk Assessment IT Audit and Compliance Data Security and Network Monitoring. Network Security, Firewall, IDS/IPS, Vulnerability Scan and Pen Test. Frameworks and Standards - PCI DSS, ISO 27001, COBIT5, NIST SP 800 SIEM Tools - Splunk, Intel, IBM Nessus Vulnerability Tool Adaptability, strong communication skills (verbal & written), organizational effectiveness, proven leadership ability, proven team work skills, demonstrated initiative. Profound knowledge of PowerPoint, Microsoft Word and Microsoft Excel

Name: David Evans

Email: ericsmith@example.net

Phone: 933-559-6280x53923