IT Analyst IT Analyst IT Analyst - Rochester Gauges Inc Work Experience IT Analyst Rochester Gauges Inc August 2014 to Present Deploy end point tools for host intrusion detection protection for centralize management Deploy network sensors to designated network locations for malicious activity monitoring Monitor activity logs and dashboards to initiate triage activities for appropriate response Review SIEM logs and perform initial incident classification following SOP Engage Team members for incident response activities and escalate per protocols Utilize ticket tracking and management system for incident resolution Perform packet capture and network traffic analysis to investigate security incidents and events Monitor Security Onion alert and event management interfaces Perform access control Windows and Unix operating systems including User account management Workstation deployment/configuration for different business units Systems review of implemented controls for internal audit assessment and policy compliance SIEM deploy and manage end point agents for SIEM data collection IDS monitor and review IDS systems alerts, review snort rule sets and tune snort configurations Monitor Security Onion consoles for activity access and initiation of analysis Configure IPS systems for network intrusion protection, - create and review rule sets for IPS performance IT Security Analyst Petra Industries Inc - Edmond, OK May 2013 to August 2014 Implement and configure DLP systems for data loss monitoring to protect sensitive/proprietary data Performa ad hoc and perform routine systems scans to redact sensitive data found in host systems Perform Host base lining and Integrity Checks for indication of potential systems compromise Perform evidence collection for potentially compromised systems following SOP Initiate IRP based on identified compromise and engage appropriate stakeholders Perform systems vulnerability assessment for regulatory and policy compliance Review vulnerability reports and engage business units in for initiation of remediation activities Track and report on compliance based on requirements provide to identify KRI/KPI Perform Disaster recovery planning, review and testing to ensure systems readiness Review and configure vulnerability scan frequency Perform systems malware analysis based on reported or known threats Review systems location and assess physical security of critical network systems Education BA in ED, CST History University of Buea Skills COBIT, GLBA, IDS, IPS, ISO Additional

Information TECHNICAL SKILLS HIGHLIGHTS Tools: Nmap, MBSA, Nessus, OpenVAS, Nessus, Zenmap, LANguard, Snort Web Inspect Networking IDS/IPS: VPN, TCP/IP, Snort, Security Onion Databases: MS SQL Server, Oracle Database Operating Systems: UNIX, MS Windows 2008 and 2012 Protocols: SSH, DNS, ARP, DHCP, SMTP, HTTPS Methodologies: Agile Scrum, SDLC, IT Project Management Regulatory Requirements: ISO 27002, FISMA, NIST, PCI-DSS, HIPPA, SOX, GLBA, COBIT Frameworks: COBIT, COSO SIEM: Splunk, Alien Vault

Name: Samuel Baker

Email: nelliott@example.org

Phone: +1-674-630-8492x2641