Security Operation Center (SOC) Analyst Security Operation Center (SOC) Analyst Security Operation Center (SOC) Analyst - Datalogic Solutions Inc New Carrollton, MD Work Experience Security Operation Center (SOC) Analyst Datalogic Solutions Inc March 2017 to Present Duties included: Perform Incident response to investigate & resolve network and system security incidents. Monitor & analyze network traffic from Intrusion detections (IDS) tools, such Splunk Express and Cisco Sourcefire. Analyze a variety 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. Review and process Accidental Disclosure requests following Standard Operating Procedures. Create SOPs for new SIEM Tools and event monitoring. Compose security alert notification and other communications. Prioritize and differentiate between potential intrusion attempts & false alarm. Develop follow up action plans to resolve reportable issues and communicate with the other analyst to address security threats and Incidents. Create incident tickets, log incidents and requests. Contribute to security strategy and security posture by identifying security gaps, evaluate and implement enhancements. Assist with the development of processes and procedures to improve incident response times, analysis of incident, and overall SOC functions. Provide Incident Response (IR) support when analysis confirms actionable incident. Strong working knowledge of network security monitoring and incident response, as well as superior written and technical communications skills Process, vet and block IOCs as needed using Cygwin 64 tool Operational Support Database Administrator Think Tech Consulting March 2015 to March 2018 Duties included: Provided physical and logical database support as needed for all the Applications specified by Client. Identified and evaluated design considerations, propose design best practices, perform database code reviews and propose performance changes. Led database issues until resolution. Serve as a liaison between the applicable third party vendor technical support team and Client if a problem case is submitted to the third party vendor. Coordinated with Application teams or other teams to resolve database issues even though the issues are not directly related to the databases. Performed database housekeeping designed to ensure that the databases are functioning optimally and securely. Maintained compliance with Client Standards

and Client Rules, including those related to the databases (e.g. access management, direct grant, db links, etc.). Performed performance tuning and/or stress testing in the non-production environment for application releases as necessary to ensure database infrastructure is configured optimally. Provided after business hours and weekend support in Client's production and contingency environments in accordance with the applicable Application release schedules. In addition, provided on-demand support for the lower environments as requested by Client Maintained the databases to meet performance standards, maximize efficiency, and minimize outages Monitored database usage, transaction volumes, response times, and concurrency levels, and measure and report its performance against the applicable Service Levels. Generated reports based on the data in the databases and reports related to the performance and integrity of the databases. Developed/maintained/enhanced database monitoring scripts designed to ensure the stability, security, and performance of the database queries. Participated in production issues as requested by other support teams or the Enterprise Command Center. Provide periodic updates on production outages and slow response issues as each incident occurs. Performed database shutdowns and restarts, troubleshooting, and database recovery. Generated performance reports (e.g., Oracle AWR report, etc.) as required for database troubleshooting. Performed system/parameter changes, reorganizations and update/gather statistics to optimize performance when required. Documented all of the required artifacts in the tickets to comply with the Client-approved change/incident/problem management policies. Monitored Database refresh processes to ensure databases refresh with the latest backups Supported all application deployments, verify deployment artifacts from the Application Maintainers, verify the service code and execute scripts. Monitored day-to-day alerts and search for solutions promptly. Created, modified and deactivated user accounts; assigned and monitored user access rights Education Bachelor's Degree University Of Yaound Skills FIREWALLS, NETWORKING, REMEDY, TCP/IP, DLP, IDS, IPS, NESSUS, SPLUNK, WIRESHARK, SECURITY, TCP, LINUX, SOLARIS, UNIX, OPEN SOURCE, JIRA, MS OFFICE, SYMANTEC, EXCEL Certifications/Licenses Oracle Certified Associate 2015 Mongodb 2015 Scrum Master 2019

Name: Robert Pittman

Email: matthew43@example.com

Phone: 001-356-620-6892x5676