Guardium Database Security Administrator Guardium Database Security Administrator Guardium Database Security Administrator - Tech Consulting Inc ? Installed and Configured Guardium Central Manager, Aggregators Collectors ? Upgraded Guardium appliances from 10.1 through 10.6 ? Installed Guardium STAP agents on database servers to implement Database Activity Monitoring (DAM) of Oracle, Exadata, SQL Server, Hadoop, and Mongo DB DBMS. ? Upgraded Guardium agents (GIM & STAP) from 10.1 through 10.5 ? Downloaded patches (Sniffer, GPU, dbs, Healtcheck) from Fix central and applied to all Guardium appliances Enterprise-wide. ? Installed Guardium policy with associated rules appropriate for meeting HIPPA and SOX requirement for DAM. ? Configured and scheduled Guardium appliance backups (system configuration and data) to backup servers ? Configured and scheduled collectors export to aggregators and import by aggregators ? Coordinated database PHI classification based on HIPPAA requirements, identified PHI fields were then loaded to Guardium for use in monitoring ? Coordinated with the DBA team to implement Guardium data-sources which were then used to implement Entitlement reporting. ? Experience implementing Oracle Database Auditing and other security features like setting profiles and strong password function. ? Coordination amongst different stakeholder groups within the enterprise necessary to implement the database security solutions in group, Unix, cyber security, network and various application owners. ? Coordinating the enterprise effort for data encryption using technologies such as TDE for data at rest and network encryption for data in motion. ? Coordinated the Activation of ATAP on 200 database servers where databases had network encryption enabled. ? Developed and maintained System Security Plans (SSP), Contingency Plans, Incident Response Plans, Disaster Recovery Plan, account management plan for all systems and conducted Privacy impact analysis. ? Conducted Categorization and classification of information to determine risk level associated with the information system, the required controls to be to ensure Confidentiality, integrity and Availability of the information system. ? Performed information System security Risk Assessments, Security Control Analysis, and risk mitigation to minimize security impact on information systems. ? Initiated Nessus Vulnerability scans, analyzed the scan report, prioritized vulnerabilities and collaborated with the system administrators to remediate weaknesses

in the information system. ? Provided weekly security status of information systems and vulnerability management reports to the Chief Information Security Officer and the System owners. ? Hands on experience in database installation, administration, configuration, production support, upgrades, patches, performance tuning, backup and recovery, space management, database security, cloning,migration. ? In-depth knowledge and understanding of Oracle Database features such as RMAN for backup and recovery, Export/Import, Data Pump and Data Guard. Working knowledge of Auditing and Database Security. ? Excellent written and verbal communication skills. ? Strong interpersonal skills and organizational skills. Work Experience Guardium Database Security Administrator Tech Consulting Inc - Laurel, MD July 2017 to Present Architect and infrastructure design for the deployment of Guardium Database monitoring solution for the entire enterprise. ? Build Guardium appliances (Central Manager, Aggregators, collectors) ? Coordinate with other teams to implement encryption solutions enterprise-wide on all databases. This involves implementation of encryption of data at rest (TDE) and data in motion (network encryption) across various database management systems such as Oracle, EXADATA MS SQL server, ? Deploy and setup configuration for IBM Guardium to ensure collectors, aggregators, load balancers, agents (S-TAP, Guardium Installation Manager (GIM), and ATAP) are properly installed. ? Develop and ensure Database Activity Monitoring policies/rules are setup in accordance with HIPAA and SOX regulation. ? Run, test and validate Guardium configuration settings and fully document technical and procedural requirements ? Develop new approaches to ensure compliance with standards and identification of security anomalies through automation and implementation of enterprise database monitoring capability. ? Implementing Guardium on various DBMS such Oracle, Sql Server, Exadata, Hadoop ? Maintain Guardium infrastructure such patching appliances, upgrading STAP agents ? Working with application owners to develop and implement monitoring and reporting use-cases. ? Implement application user translation for out of the box application such as Peoplesoft etc. ? Implement Sensitive data and database discovery configuration ? Install Guardium STAP agents on database servers to implement Database Activity Monitoring (DAM)on including Oracle, Exadata, SQL Server, Hadoop, MongoDB, ? Upgrade Guardium agents (GIM &

STAP) from 10.1 through 10.5 ? Coordinate the Activation of ATAP on 200 oracle database servers where databases had network encryption enabled. ? Download appliance patches (Sniffer, GPU, alerter etc.) from Fix central and applied such to all Guardium appliances enterprise wide. ? Install Guardium policy with associated rules appropriate for meting HIPAA and SOX requirement for DAM. ? Coordinate enterprise effort for data encryption using technologies such as TDE for data at rest and network encryption for data in motion. ? Experience using Shell Scripting to automate database jobs such as backups, ETL jobs using sql Loader, Materialized view refresh in Unix based environments. ? Experience using PowerShell Scripting to automate database jobs such as backups, ETL jobs using sql Loader, Materialized view refresh in windows environments. ? Configure and schedule Guardium appliance backups (system configuration and data) to FTP sites ? Configure and schedule collectors export to aggregators and import by aggregators ? Configure integration with Qrader, our SEIM tool. ? Coordinate database PHI classification based on HIPAA requirements, identified PHI fields were then loaded to Guardium for use in monitoring ? Coordinate with the DBA team to implement Guardium data-sources which were then used to implement Entitlement reporting. ? Familiar with IT Regulations, PCI / Sarbanes-Oxley / Privacy laws ? Ability to work independently, leading meetings with application and development teams discovering and documenting detailed requirements ? Ability to plan, coordinate and implement Guardium agent installations during nighttime maintenance windows Skill sets Lead IT Security Analyst Telesis Corporation - McLean, VA December 2016 to July 2017 Implemented Risk Management Framework (RMF) in accordance with NIST SP 800-37. ? Utilized NIST SP 800-18 to develop and update System Security Plans. ? Collaborated with ISSO's/System Administrators in remediating security findings ? Analysis and prioritize Nessus Scan results from Critical, High, Moderate and Low and ensured remediation of vulnerabilities from critical to low vulnerabilities. ? Provide System Owner and CISO with weekly, monthly and quarterly POAM reports. ? Ensured security policies, procedures; recommendations comply with FISMA, NIST and Fedramp, Organizational guidelines and technical best practices to protect the CIA of Systems. ? Responsible for development and maintenance of system security plans and contingency plans, Privacy impact analysis, account

management plan for all systems. ? Developed Plan of Action and Milestones (POA&M) for identified vulnerabilities and ensure compliance through updates as mitigation progresses until closure of POAM. ? Organized meetings with Assessment team and other stakeholders to plan for Assessment and reassessment of information systems. ? Performed Risk Assessment in accordance to NIST SP 800-30 Rev 1. Determine and prioritized vulnerabilities for remediation based on impact to information systems. Information System Security Officer NuAxis Innovations Virginia April 2016 to November 2016 Collaborated with assessors to provide artifacts and other documents as required. ? Updated security policies and ensured that procedures are in place and rightly implemented. ? Maintained inventory of all information Security System and respond to data calls. ? Monitored Authorized Information System using NIST 800-137 guidelines. ? Performed Risk Assessment in accordance to NIST SP 800-30 Rev 1. ? Reviewed and ensured Privacy Impact Assessment document after positive is created IT Security Analyst / Compliance Infos Pro Solutions, Maryland May 2013 to March 2016 Advised Information System Owner (ISO) of security impact levels for Confidentiality, Integrity and Availability (CIA). ? Utilized NIST SP 800-18 and update System Security Plans from SP 800-53. ? Collaborated with ISSO's in remediating audit findings, security planning and reporting, and mitigation of security vulnerabilities are completed in a timely manner. ? Monitors, evaluates and report on the status of information security system and directs corrective actions to eliminate or reduce risk. ? Initiated compliance and vulnerability scan request to identify and report weaknesses and potential security breaches. Junior Oracle Database Administrator Woodley House Inc - Washington, DC January 2011 to April 2013 Managed and supported multiple 9i. Oracle 10g, 11g, databases. ? Created and cloned Oracle Databases on ASM. Performed database cloning and re-location activities. ? Maintained data integrity and created users, managed profiles, resources and password security. ? Upgraded Databases from lower version to higher version. ? Tuned SQL statement against database and its objects. ? Installed and tested new versions of Oracle database, applications, and patches. ? Performed and validated backups, performed restores and recoveries, refreshed databases and applications Education Bsc in Cyber Security Management and Policy University of Maryland University College 2018 Skills

DBA, MYSQL, Sql Dba, Sql Server, Oracle Dba Certifications/Licenses Oracle Certified Associate December 2014 to Present Certified Oracle Database Administrator - 11g ? IBM Certified Administrator - Security Guardium July 2019 to Present IBM Guardium Security Administrator - V10.0 ? Cloud Security Alliance Certificate of Cloud Security Knowledge August 2017 to Present Cloud Security Knowledge.

Name: Andrea Trevino

Email: johnjarvis@example.org

Phone: (670)744-5020x1632