Cyber Security Analyst Cyber Security Analyst Cyber Security Analyst - CMCI Corporation Work Experience Cyber Security Analyst CMCI Corporation - Fairfax, VA August 2018 to Present Primary Responsibilities Includes: ? Developed Requirement Traceability Matrix (RTM) to document the results of the assessment ? Met with the system team to collect evidence, develop test plans and procedures and document test results. ? Worked closely with Oracle support on different Oracle vulnerabilities issues ? Performs comprehensive Security Control Assessments (SCA) and wrote reviews of management, operational and technical security controls for major applications and information systems. ? Regularly work with the technology teams to ensure their Authentication-Authorization processes are up to date and meet guidelines, including segregation of duty. ? Experience with server, database, application scanning using Nessus tools ? Experience in vulnerability Management, Monitoring, identification, analysis and remediation of network vulnerabilities. ? Develop, review and update Information Security System Policies, System Security Plans (SSP), and Security baselines in accordance with NIST, FISMA, OMB, NIST SP 800-18,NIST 800-30,NIST 800-39 and industry best security practices ? Examined events logs for irregularities. Identified irregularities are then reported as incidents. Then incident response is then initiated to mitigate these irregularities. ? Develop ATO packages for systems that need to go through the A&A process to obtain an ATO. ? Experience with STIGS and analyze all the security vulnerabilities on the database server , application and operating systems. ? Perform end-to-end Security Control Assessment, with in-depth experience in NIST SP 800-53A &37. ? Access and communicate security risks associated with development practices in an organization. ? Design and implement a risk mitigation strategy to foster organization cyber resilience. ? Analyze vulnerability and compliance scan results and work with stakeholders to ensure vulnerabilities are remediated and system configurations meet hardening standards. ? Host and facilitate kick-off meetings and presentations with system clients on the operational security posture for assigned systems and on security related requirements ? Working knowledge of the Risk Management Framework (RMF) with the 6 Step require for Authority to Operate (ATO) process ? Assisted with the review and update to security artifacts such as SSP, SAR, SAP, SOP, CP, PIA and PTA required for information

systems to be granted an ATO ? Conducted security awareness training and expected rules of behavior for end users. ? Researched security enhancements and make recommendations to management. ? Conducted Risk assessment and provided recommendations for RMF system reviews. ? Supports the government customers business activities related risk identification and measurement systems within various technical and usage boundaries ? Supports development and documentation of Security Architectures, Roadmaps, and investments. ? Reviewed security controls and provided implementation responses as to if and how the systems are currently meeting their security requirements. ? Supported the team tasked with the review of security artifacts, assessment reports, and ATO memos for proper implementation and compliance with applicable policies and standards Cyber Security Analyst Synergetic Information Systems Inc - Washington, DC January 2015 to July 2018 Primary Responsibilities Includes: ? Experience with Security Assessment & Authoring Process (SA&A) and preparing ATO package documents such as the SSP, SAR and POA&M. ? Develop ATO packages for systems that need to go through the A&A process to obtain an ATO. ? Experience with server, database, application scanning using Nessus tools ? Track and update POA&M for correction actions following assessment activities and in response to identified vulnerabilities for maintaining system ATO status. ? Experience with scanning Window, Linux, Macos using Wireshark tools. ? Experience with protecting the confidentiality, integrity and availability of sensitive and critical information system as well as assist refining and clarifying security requirements. ? Monitored security logs, analyzed data to identify potential threats, violations and breaches ? Responded to identified and reported security incidents ? Evaluated technical issues of partner and customer contracts and provided analysis to legal team ? Promoted security awareness and educated the staffs ? Track and update POA&M for correction actions following assessment activities and in response to identified vulnerabilities for maintaining system ATO status. ? Experience in developing and reviewing A&A security artifacts including but not limited to Incident Respond Plan (IRP), Contingency Plan (CP), Privacy Threshold Assessment (PTA) and Configuration Management Plan (CMP). ? Strong verbal, written, and interpersonal skills with the ability to solve problems individually and collaboratively. ? Experience with STIGS and

analyze all the security vulnerabilities on the database server , application and operating systems ? Develop list of IOC's and update blocking/monitoring tools as appropriate. ? Reset password of compromised user accounts, contain and reimage infected systems. ? Monitor AV tools for indications of infected systems and act accordingly to contain and remediate threats. ? Conducted Risk assessment and provided recommendations for RMF system reviews. ? Develop meaningful dashboards to easily spot real threats in the environment. ? Push policy and agent updates to endpoints that are out of compliance. ? Retrieve log files for analysis and remediation response. ? Threat Hunting - Investigate suspect endpoint or user behavior. ? Examine logs from a SIEM regarding particular user ID or endpoint related to an event RDBMS Tech 2012 to 2016 Databases: Microsoft SQL Server 2005,2012,2016 , 2017 ,Oracle 12cR2 , Oracle 11gR2, 11gR2 RAC, Oracle10g, STIGS, Nessus, OpenVAS, Nikto, Wireshark ? Tools: TOAD, OEM, Grid Control, SQL*Loader, RMAN, Shell Script, AWR, ASH, Toad, Cron jobs, SQL*Loader, OEM, RMAN, SRVCTL, DBCA, ? RDBMS Tech: Oracle 10g, 11g,12c Standby Database, SQL Server ? Tools and Utilities: Export/Import, RMAN, Data Pump , WinScp, ASM, PUTTY,VNC ? Languages: Shell Scripting, SQL and PL/SQL. ? Operating Systems: UNIX, LINUX, SOLARIS, Windows Server ? Networking: Wireless/Virtual Local Area Network (WLAN, VLAN, LAN), Wide Area Network (WAN) TCP/IP, Virtual Private Network (VPN), Storage Area Network (SAN), Network Attached Storage (NAS) Database Administrator Technatomy Corporation - Fairfax, VA January 2011 to January 2015 Primary Responsibilities Includes: ? Implement the Installation of 10g,11g ,12c Oracle database , upgrade, migration, Storage Allocation, Backup & Recovery, Replication, Performance Tuning, Configuration/Installation of Oracle databases using oracle technologies such as Data Guard, RAC, ASM, and Advanced Security on the database. ? Experience in implementation and configuration of Oracle , 10g, 11g and 11gR2 and 12c Standby Databases. ? Administration of Oracle Enterprise Manager (OEM) on 12c and 13c ? Implement the installation of the Oracle Data guard database and administer it on 10g,11g, 12c both on RAC, single instance and standalone ? Managed Database Structures, Disk Spaces, Storage Allocations, and table's constraints, Database Access, Roles and Privileges. Creating Users and Roles ? Managing Database Structures, Storage

Allocation, Table/Index segments, Rollback segments, constraints, Database Access, Roles and Privileges and Database Auditing on all 10g,11g, and 12c ? Experience in using various SQL Server Tools like Enterprise Manager, Management Studio, Query Analyzer, Profiler, SQL Server Agent, DTS, SSRS, SSAS and SSIS. ? Experience in SQL Server 2005, 2008,2012,2016 Installation, Configuration of Stand-alone with multiple instance in Clustered and Non-Clustered environment. ? Experience in high availability SQL Server Solutions that includes Mirroring and Clustering ? Administration of ASM DISK management (creating disk group, adding/removing disks to disk-groups) on 10g,11g, and 12c ? Experience in Managed ASM Disk groups in oracle RAC and standalone ? Worked closely with Oracle support on different Oracle issues ? Experience to work on OS level clustering mechanism for Oracle database with ASM on 10g,11,and 12c Oracle Database Administrator Soft Tech Consulting January 2009 to January 2011 Primary Responsibilities Includes: ? Handled operational responsibilities like database refreshes, backup and recovery, security, documenting standards and procedures, data migration, data clean-up, data archiving on oracle 10g,11g and 12c etc ? Responsible for Replication and Mirroring related issues on SQL server 2012,2014 and 2016 ? Export and Import of Database using pump utility on oracle 11g and 12c ? Proficient in use of tools like extended events, DMVs, SQL Server profiler and Windows performance monitor ? Install and configuring MSSQL 2008 Server stand alone ? Experience with Virtualization technologies such as installing, configuring, and administering VMware ESX/ESX 6 5.5, Red Hat environment ? Experienced with Linux family (Red Hat Enterprise Server, Cent OS). ? Creating templates for Linux VM's used for deploying for the environments. ? Performed regular installation of patches using YUM, and RPM utilities and remotely copying files using vsftpd, scp,and winscp ? Hands-on experience in diagnosing, troubleshooting various networking, hardware & Linux/ UNIX server issues, performing preventive maintenance ? Set up and administer user and groups accounts with restricted permissions ? Installed and configured Logical Volume Manager - LVM ? Experience in systems patching Linux OS, kernel tuning and resource management for Oracle databases alongside DBA's in team ? Experienced with TCP/IP networking tool using them in network configuration, maintenance and troubleshooting ?

Experience installing and configuring UNIX server on the Solaris and centos platforms and introducing the server to the network ? Expertise in Installation, Configuration, Trouble-Shooting and Maintenance of Red Hat Enterprise Linux, CentOS in physical and virtual Linux servers ? Experience in applying critical patches (CPU/PSU, Security Patches) on oracle 10g,11g and 12c Oracle Database Skills Summary: Education Masters of Science in Health System Management in Health System Management University Of Baltimore - Baltimore, MD May 2012 Bachelor of Science in Criminal Justice in Criminal Justice Coppin State University - Baltimore, MD May 2009 Boltos Solutions Institute Skills Database, Sql server, Oracle, Sql, Security, Nessus, Wireshark, Linux, Authentication, Cyber security, Active directory, Ssa, Ec2, Life cycle, Risk assessment, Dod, System security, Auditing, Federal government, Government contract Additional Information Skills: ? Experience working with Government contract such as SSA, VA IAM contract and DoD. Focusing on the database tasks by documenting SOP , explaining database issues to the client and how to improve it. ? Experience with Linux, Oracle Database and SQL Server. ? Experience in the system life cycle project management and Security Assessment & Authorization (SA&A) ? Experience with Microsoft Active Directory and how it works ? Experience with AWS Cloud , with techniques such as EC2, S3, VPC, RDS, ELB, SNS, AMI,IAM, KMS, Route 53, and Cloud Watch ? Experience with Agile methodologies ? Previous federal government contractor experience on Cyber Security and Auditing the systems ? Experience with server, database, application scanning using Nessus tools ? Experience with window, linux , Macos server scanning using Wireshark tools. ? Experience with system security documents, and POAM Management. ? Experience with Risk Assessment and Authorization and Authorization-To-Operate (ATO) Process. ? Setup secured password less SSH authentication on servers using SSH keys. Setup SSH keys for secured key-based authentication. ? Experience with Security Controls Assessment and Policy Procedures. ? Experience with Cyber Security Framework (RMF) ? Experience with Patching the systems to fix any vulnerability both on Linux and Windows.

Name: Lori Ellis

Email: aarondecker@example.com

Phone: 001-268-247-2758x6655