IT Security Analyst-CA-MMIS IT Security Analyst-CA-MMIS IT Security Analyst-CA-MMIS - Conduent A Systems Security Analyst with a wide range of experience built from working with diversified systems. Extensive experience built from Infrastructure and Operating systems deployment and management. As well as NOC and SOC experience with deep focus on Security monitoring and analysis with multiple SIEM and other Security tools. system administrator with years of IT experience in Installation, Administration, Configuration and Technical support in Unix (AIX, Solaris) and Linux (Redhat, Ubuntu, Suse) infrastructure. Work Experience IT Security Analyst-CA-MMIS Conduent March 2019 to Present California Medicaid Management Information System) Responsible for analyzing customer requirements for audit and risk assessments (SRA's) Responsible for database control and/or end user support of established system controls Ensure system controls and security are in place and determines operation consistency with SOP Participate in security testing, analyzing and documenting test results/risk to provide counter measures Maintain System Security Plans (SSP's)for assigned networks/systems and conduct periodic reviews Perform monthly vulnerability scans and work with operations team to remediate results Review and reports threat analysis and provide input on overall system process Work with clients internal/external and vendors on secure and confidential plans (SCP) Coordinates with system owners, data owners and service providers to maintain all security documents Conduct interviews with developers and project management to assess systems against assurance policies Installation, configuration and deployment of Database monitoring tools Respond and investigate system alerts for various IPS/IDS systems Initiate and review outstanding POA&M and gather supporting evidence for their closure Tools: Nessus, Wireshark, Acunetix, Imperva, Rapid7 IT Security Analyst ScienceLogic March 2018 to March 2019 Perform incident triage and track investigations through enterprise ticketing system Assist with remediation reviews and implementation of remediation plans Report on compliance and vulnerability metrics for management review Modified vulnerability assessment frequency and perform ad hoc assessments as needed Monitor systems traffic and perform packet capture for further analysis and review Participated in evaluating and troubleshooting security solutions and new IT infrastructure systems Review reports and establish a patch management plan for known vulnerabilities Monitor security systems and review threat intelligence data for critical/known vulnerabilities Configuration and deployment of enterprise vulnerability management and assessment tools Tools: Nessus, Wireshark, CUspider, PfSense, Splunk, SL1, ZenMap, LogRythm Security Analyst June 2016 to March 2017 Follow standard operating procedure and policies in administering environmental support Systems Monitoring and incident assessments to determine threat response Configuration and deployment of vulnerability assessment tools within the Oracle cloud platform Review SIEM logs to determine appropriate remediation and derive remediation plans Fulfill service request from internal and external customers surrounding the security of Oracle Cloud Configuration and management of IDS and IPS systems for host and network defense Monitor and review alerts for investigation and classification and resolved issues following SOP Worked with DevSecOps in stress testing and benchmarking for the cloud network Interface with clients for problem analysis and review of active incidents and response plans Documentation/review of incident response plans as well as Standard Operating Procedures (SOP) Environment: RHEL, Oracle linux, Oracle virtual box, VmWare, Bash, TCP/IP, Oracle Database, Ngios. Cyber Security Analyst Deutsche Bank August 2015 to June 2016 Monitor security systems and review incidents/events for IOC Perform post incident analysis and analysis for tracking and investigation Performed root cause analysis, vulnerability assessments of system Provided support on weekends and after hours Participated in various penetration testing activities with pen testers and security architects, Installed and configured various security management monitoring tools Updates and documented security procedures in confluence and various risk records Participated in lesson learned meetings with upper management Assessed security risks and communicate them to systems administration for strategic patching Interface with clients for problem analysis and review of active incidents and response plans Monitoring and analysis of network packets on various systems for anomalies Environment: RHEL, Sql, Microsoft Server, Tools: AlienVault, Nessus, MSBA, ZenMap, Splunk Systems Administrator Wal-Mart February 2011 to April 2015 Installation and configuration of AIX servers Performance monitoring of AIX/ Linux servers and user management Creation of logical partitions using and replacing broken disk on AIX/ Linux servers Created and maintained DLPAR by HMC on the pSeries servers according to the resources demands Experience in the building LPAR and making them VIO Servers and VIO clients and mapping Installation, upgrade, configuration, fail over/fail back testing for HACMP 5.4 Building of Virtual machines using Vmware Esxi 5.5 and installing Centos 7 on them and monitoring Good knowledge of Logical Volume Manager, created and maintained volume groups, physical volumes Environment: AIX, RHEL, Suse, Bash, TCP/IP, Nagios, Worked on TCP/IP configuration, IP address assigning, network interface configuration, static routes Troubleshooting and monitoring OpenStack through various log files Redhat Linux System Administrator ICF International - Fairfax, VA June 2009 to January 2011 24x7 Support on a weekly rotation basis to ensure availability of Servers. Performance monitoring and capacity management on Redhat Linux servers. Involved in the administration of backup on the Redhat Linux servers Network troubleshooting and diagnosis of root cause analysis Daily management including File System issues, performance tuning. User Account Management and password reset Installation and confirmation of the maintenance patches, installation and updating of the new software Assist Application department to install application on Redhat Linux systems and tuning for Application Documenting changes and Configuration of Systems and keep it current. Installation and maintenance of JBoss middleware. Utilize SQL statements SELECT, UPDATE, INSERT, to update and maintain Sql Database Environment: RHEL, SQL Database, Windows, VmWare, TCP/IP, Bash Jr. Redhat Linux System Administrator Fannie Mae - Reston, VA January 2006 to January 2008 Installation of packages using Yum and Redhat Linux package manager on servers Installation and configuration of Apache server on Linux environment Maintaining User Account by changing permission, password etc. Performed root cause analysis on failed components and implemented corrective measures Troubleshooting of the system for startup problems, network and hardware issues Creating and Maintaining File Systems according to the required size Creation and administration of Virtual Machines using VMware, Hypervisor Used LVM for the management of logical volumes including creation of physical volumes in Linux Built virtual machines with Microsoft Hyper-V and Vmware 6.0/6.5 and installed proprietory software Environment: Microsoft Hyper -v, VmWare, RHEL, Sieble, Windows, Bash scripting Education BSc in Pharmaceutical Marketing /Management University of the Sciences - Philadelphia, PA May 2001 Skills Hipaa, Ids, Ips, Nessus, Nist, Nmap, Pci, Siem, Snort, Splunk, Tcpdump, Wireshark, Dhcp, Network monitoring, Tcp, Tcp/ip, Aix, Linux, Solaris, Unix

Name: Dana Graham

Email: rogersmartha@example.com

Phone: 417-609-1990x757