Cloud Security Engineer Cloud Security Engineer Cloud Security Engineer - Affinity E Solutions Lorton, VA Work Experience Cloud Security Engineer Affinity E Solutions - Alexandria, VA September 2018 to Present   Administration of cloud computing environments and servers with Amazon Web Services Gov. (EC2, S3, Route 53, IAM, RDS, Certificate Manager, Amazon aLB, Amazon Connect)   Applying windows patches to all of cloud environment utilizing WSUS. Ensured that all server hardware, operating systems, software and procedures aligned with DOD standards and strategic business plan.   Conduct Vulnerability Scans of the entire network and servers via ACAS and Nessus Tenable.   Maintain Enterprise Cyber Security for DOD network using McAfee Host Based Security System (HBSS)   Analyze Security Scanning results to identify critical flaws in applications and systems.   Performed continuous sync operations, including branch strategy planning, resolving conflicts and sync damage analysis in .NET framework, ensuring success of release cycles.   Server and network administration in corporate datacenter and Amazon cloud.   Client support for Windows Server 2016 and Server 2012 R2 on multiple networks supporting Web administrators, Database administrators and Infrastructure team.   Creating, implementation and maintaining of Group Policy Objects.   Create SSL certificates through Certificate Manager in AWS and configure on all appropriate load balancers.   Managed and performed production builds 24/7 as requested to meet critical business needs.   Managing and implementing configuration baselines following industry standards and knowledge of security implementation guides (DISA STIGS, Manual SCAP tool checks)   Using Nessus Vulnerability scanning tool to remediate open vulnerabilities.   Installation, Administration and maintenance of SQL Server Instances, setting up differential and full backups for databases in SQL.   Create users and assign permissions based on level of database access user would need.   Monitor backups on production environment as well as test environment.   Using Alien Vault to manage cyber-attacks and to remediate any cyber related issues.   Monitor system configuration and user access/privileges to ensure data integrity. Network/ Systems Admin CSRA - Washington, DC June 2017 to September 2018   Provided IT Support for 865 CNCS employees remote and local. Encrypted and Decrypted full disk encryption drives using Checkpoint.   Administration &

management of Microsoft O365 users account, migrating users from on-perm server to O365. SharePoint troubleshooting, migrating files from share drive to SharePoint updating permission for users.   Manage, lead and support Windows 7, 8, 8.1, 10.   Configure, image, deploy, and integrate new equipment into the environment.   Resolve issues related to Windows, application, virus isolation, and removal, storage and hardware configuration problem.   Install latest versions of Operating Systems on demand, per requirements of the clients.   Migrate users from Windows 7 to Windows 10.   Maintain different group policies for all 35-organizational unit in Active Directory. Configured and maintained VOIP phones using Cisco Call Manager.   Identified vulnerabilities, recommended corrective measures and ensured the adequacy of existing information security controls.   Configure port security on 32 CISCO switches using Secure CRT.   Group Policy Object (GPO) creation, troubleshooting, and management through Active Directory.   Server administration in Microsoft (MS) Windows environments, including MS Windows Server 2008 R2 and 2012 R2 to include performance monitoring, tuning, patching and security updates.   Assisted with testing and implementing Microsoft and native applications.   Process requests for access control and for group drive mappings via login script.   Verify new software deployments and GPO policies work by testing them in a test domain as appropriate.   Monitored and evaluated tickets through Remedy Salesforce.   Created rules through Palo Alto to block any suspicious ports, IP address and websites.   Conducted base level analysis to determine the legitimacy of files, domains and emails.

   Ensured that all server hardware, operating systems, software and procedures aligned with organizational standards and strategic business plan.   Complete security assessments for new hardware and software: lookup CVE's and apply remediation.   Install, troubleshoot and apply patches to Crystal Reports.   Develop and deploy Adobe Creative Cloud Suite packages. Mid-Level Systems Administrator Chenega Corporation - Chantilly, VA August 2014 to June 2017   Provided 24/7 support to end users by email, phone, tickets and in person.   Actively researched and learned about new technologies to improve current workflows.   Prepared conference room technical systems per request of senior management.   Provided users with steps to help resolve issues. Tracked and recorded tickets for future references.   Proficient in the use of Microsoft Service

Manger ticketing system.   Monitored and resolved tickets to remain compliant of the Service Level Agreement (SLA).   Maintained adequate stock of approved government supplies.   Prepared hardware/software for new hires.   Accessed service tickets per request using Service Now facility response system. Education Bachelor's in Applied Information Technology in Applied Information Technology Strayer University June 2018 Skills Tcp/ip, Splunk, Wireshark, Sharepoint, Tcp, AWS Links https://www.linkedin.com/in/sali93 Additional Information ACQUIRED SKILLS   Understanding of PCAP analysis through Wireshark application.   Understanding of security applications such as Splunk and Sourcefire.   Understanding of the OSI and TCP/IP model, common protocols and ports.   Proficient with IPv4 addressing scheme.   Used AlienVault to determine known vulnerabilities and known CVE's   Experience with JIRA, Salesforce and SharePoint.

Name: Kelly Benson

Email: steeledaniel@example.net

Phone: 292.495.6590