**SUMMARY OF QUALIFICATIONS**

Proven technical and leadership experience in the following areas: Cyber Security, IT Management, Cloud Infrastructure, network configuration and maintenance, configuration management, project management, network and systems security, server platforms and system Integration. I have proven experience executing roles as both team member and management in various enterprise level environments. Technologies used include Cloud Architecture and Engineering across AWS, Azure, and GCP, Pen-Testing, network monitoring, firewalls, routers, switches, Cisco VoIP devices, and Cisco Security devices

**SKILLS**

17+ Years - Manage priorities in a high paced enterprise environment.

17+ Years - Authentication & Access Control Management.

17+ Years - Team Building and Leadership.

17 Years - Network and server Operations and Maintenance.

17 Years - Microsoft Windows /UNIX/LINUX operating systems management.

17 Years - Implementing DOD DITSCAP / DIACAP IA/RMF Processes.

12 Years - Performing back-ups on both servers and networking devices.

12 Years - Disaster Recovery Planning.

12 Years - Risk Management.

10 Years - Program and Project management and development.

10 Years - Cyber Security Administration.

10 Years - Cisco Voice Administration

10 Years - ITIL Framework Experience.

10 Years - Change Management.

10 Years – Cloud Administration.

10 Years - Configuration Management.

10 Years - Stakeholder Management.

10 Years - Security Testing and Evaluation (STE).

8 Years - System Development Life Cycle

6 Years - Penetration Testing

6 Years - IaaS, PaaS, SaaS, IaC

6 Years - Cloud Architecture

5 Years – Cloud Engineering

**CLEARANCE**

Active U.S. Government TS/SCI clearance with CI Polygraph

**CERTIFICATIONS**

AWS Certified Solutions Architect – Associate – 03/18

CompTIA Advanced Security Practitioner (CASP) - 01/18

CCNA-Voice - 08/14 (Cert# 424927719621BMXI)

CEH - 07/14 (Cert# ECC13630198937)

MCITP-DA - 12/12 (Cert# E097-8575)

CCNA - 08/11 (Cert# 424927719637DOYM)

ITIL V3 - 02/10

Security+ CE - 07/09 (Cert# COMP001009138165)

Currently pursuing AWS Architect Professional Certification

**PROFESSIONAL EXPERIENCE**

**Senior Manager/Cloud Architect**

**Octo Consulting Group, Rome, New York July 2019 to present**

* Assumed role as Epic Team Lead and Product Owner for ACAS service implementation across both AWS GovCloud and AWS C2S cloud infrastructure.
* Worked with Air Force Research Lab (AFRL) AWS Cloud team to migrate DCGS(A) services to the GovCloud and C2S cloud in an Agile team environment.
* Conducted extensive Research and Development engineering efforts and delivered briefings and demos to senior leadership.
* Engineered system integration to be fully automated using CI/CD pipeline tools such as Puppet, docker, Bitbucket, AWS Cloud Formation, Jira, Kubernetes, Terraform, Git, and Jenkins.
* Integrated with security engineering DevOps team to develop ACAS/TenableSC, Elasticsearch (ECE), Consul, Concourse, Vault, and ClamAV security solutions.
* Successfully migrated customer software applications into production using AWS cloud services.

**Solutions Architect**

**World Wide Technology, Fort Belvoir, Virginia Jan 2019 to July2019**

* Tanium endpoint management platform subject matter expert.
* Integrated Tanium services into ARCYBER enterprise DODIN network operations.
* Created patch management processes and documentation for using Tanium to patch enterprise endpoints.

**Expert Security Architect Consultant (Cloud Security)**

**DXC Technology, Aberdeen, Maryland, Jun 2018 to Dec 2018**

* Acting as a project manager to implement a cyber security tools migration to the ServiceNow cloud platform.
* Serve as cloud security subject matter on multiple cloud related programs.
* Leading data consolidation projects by migrating existing risk management applications into the public cloud.
* Conducting research, designing, and development of enterprise cloud security architectures.

**Cloud Security Architect**

**ICF International, Aberdeen Proving Grounds, Maryland, May 2017 to June 2018.**

* Developed architectural plans using FEDRAMP standards to migrate DOD Cyber Security Service Provider (CSSP) services into the cloud infrastructure using AWS, Google Cloud, AZURE and Oracle cloud services.
* Created the cloud formation scripts, setting up the VPC (public and private subnets) and IAM modules.
* Used IAM to create new accounts, roles, groups and policies.
* Work at optimizing volumes and EC2 instances and created multiple VPC instances.
* Designed AZURE Network Security Groups (NSGs) to control inbound and outbound access to network interfaces, VMs and subnets.
* Designed and deployed AWS Solutions using EC2, S3, EBS, Elastic Load balancer (ELB), auto scaling groups.
* Used Multi Factor Authentication to secure the AWS Account.
* Managed network security using Security Groups and Designed roles and groups for users and resources using AWS Identity Access Management (IAM).
* Utilize Cloud Watch to monitor resources such as EC2, CPU memory, Amazon RDS DB services, and EBS volumes.
* Highly skilled in deployment, configuration management, data security and troubleshooting of the applications using AWS, GCP, and Azure services.
* Designed and configured Azure Virtual Networks (VNets), subnets, Azure network settings, DHCP address blocks, DNS settings, security policies, and routing.
* Provided high availability for IaaS VMs and PaaS role instances for access from other services in the VNet with Azure Internal Load Balancer.
* Deployed Azure IaaS virtual machines (VMs) and Cloud services (PaaS role instances) into secure VNets and subnets.
* Implemented high availability with Azure Resource Manager deployment model.
* Responsible for the Provisioning of Azure Network Environments with Virtual Machines for various clients with the use of PowerShell ISE.
* Design roles and groups using Azure Identity and Access Management (IAM).
* Configured internal and internet Load balancers for Virtual machines in Azure Cloud service.
* Implemented Network traffic rules and Access Control List's (ACL) for Virtual Network in Microsoft Azure and AWS Cloud Service Platform.
* Experience in Windows Azure Services like PaaS, SaaS, IaaS and worked on Azure PaaS Blob and Block storages.

**Security Engineer (Vulnerability Management)**

**TEK Systems, Flowers Foods, Thomasville, Georgia, March 2017 to May 2017**

* Implemented an architecture plan to stream-line the functionality of the in-production Tenable Nessus vulnerability scanners and Nessus Security center in a SOX, PCI, and HIPPA environment.
* Conducted regular scheduled scans, PCI, CIS, and remediation scans and created detailed reports of the findings.
* Operated IBM QRader SIEM tool to detect vulnerabilities and threats across the network.
* Architected the integration of the Cyber Ark credential tool and the Nessus Security Center to manage all credential accounts for Nessus.
* Developed a VMware Cyber Test Lab environment to test new software before moving to production.
* Conducted configuration analysis of the SonicWall firewalls in preparation to migrate to Palo-Alto Firewalls.
* Created detailed documentation and Standard Operating Procedures for vulnerability analysis, Vulnerability Remediation processes and architecture road mapping.
* Conducted ForeScout CounterAct analysis and configuration as a NAC and an Intrusion Detection System (IDS) in the network environment.
* Developed detailed documentation for or the vulnerability management Program in preparation future SOC Implementation in the company.

**Technical Program Manager/ Lead Cyber Operations Developer**

**Silotech Group,** **Fort Gordon, Georgia 30905, Oct 2015 to March 2017**

* Promoted to remote Technical Program Manager and assumed led over two active Cyber training/development contracts on Fort Gordon
* Lead for Cyber Common Technical Core (CCTC) Cyber Operations Development team.
* Provide direct supervision and performance management of program staff. Conduct annual performance evaluations for staff.
* Designed, developed and implemented courseware that supported large blended solutions as well as Directed the Development and implementation of course curriculum for the United States Army 17 Series MOS Cyber Common Technical Core (CCTC) with a focus on Cyber Protection Team mission requirements single course events
* Implemented a change management process for all ongoing major and minor changes.
* Developed Advanced Practical exercises and Cyber tools with Python, C, and PowerShell to provide optimum hands on experience.
* Proficient in network exploitation, cyberspace defense, cyber operational preparation.
* Working knowledge of advanced persistent threat methodologies.
* Perform application and network penetration testing by identifying and exploiting network and application level vulnerabilities in order to illustrate risk.
* Proficient in Amazon’s AWS, EC2, IAM, VMware’s ESXI, VSphere 6.0, Vcenter, VSAN, VRealize, and NSX technologies.

**Cloud Security Engineer**

**Creative Business Solutions, CYBERCOE G6, Fort Gordon, Georgia 30905, Oct 2014 to Oct 2015**

* Served as lead Cyber Cloud Security Engineer
* Creating a secure Infrastructure as a Service (IaaS) and a Service as a Service (SaaS) platform using VMware hypervisor, and AWS EC2 cloud platform, IAM and certificate manager.
* Provided CND network traffic analysis using various network monitoring tools.
* Network security planning and implementation for TRADOC new Cyber campus area network.
* Conduct penetration tests on systems and applications using automated and manual techniques with tools such as Metasploit, Burpsuite, Kali Linux, many other open source tools as needed.
* Work with support teams to address findings as a result of any Vulnerability tests Cyber Datacenter network connectivity design and implementation.
* Performed application penetration testing on thick client, and other types of applications to identify significant vulnerabilities that threaten customer systems.
* Conducted network scans using NMAP, WMAP, and ZenMap to locate systems vulnerable to attacks.
* Administered and scanned the network with Nexpose, OpenVas, and Nessus/ACAS Scan Engine.
* Conducted packet analysis and generated output files using Wireshark and TCP Dump
* Performed research to identify potential vulnerabilities threats to existing technologies and provided an accurate notification to management of the risk potential and options for risk remediation.
* Perform implementation of DISA STIGS on devices designated for the army datacenter consolidation effort.
* Designing a functional virtual DMZ within a virtual VMware environment.
* Conducted in depth Vulnerability Assessment and Risk Assessment using Risk Management Framework (RMF) security processes.
* Proficient in VMware’s ESXI, VSphere 6.0, Vcenter, VSAN, VRealize, and NSX technologies.

**IT Specialist (Network/Information Security Engineer)**

**U.S. Government**, **7th Cyber Protection Brigade, Fort Gordon, Georgia 30905, May2014 to Oct 2014**

* Working knowledge of Network Scanning, Network Exploitation, and Network Defense as a CND Threat Mitigation member of a Cyber Protection Team (CPT).
* Conducted mission protection, discovery, and counter-infratration using Red team/Blue team/Hunt methodologies.
* Conducted extensive hands on training in Vulnerability Assessment and Networking and Packet Analysis.
* Hands on experience with Nessus Vulnerability Scanner, and Security Onion Intrusion Detection System.
* Hands on knowledge of CND network traffic analysis using various network monitoring tools.
* Performed CTF exploitation practices, passive & active host discovery.
* Improved proficiency with scripting languages such as PowerShell, Python, Java script, and Perl script.
* Performed both IDS and IPS threat detection and mitigation and generated custom IDS rules.
* Performed software threat analysis and digital forensics data analysis.
* Working knowledge of Cryptography, Authentication, mitigating threats, and User and role-based security.
* Performed buffer overflow protection, defeat and exploitation, and generated shell code.
* Hands on penetration testing experience with Kali Linux and Metasploit exploitation tools.
* Performed Linux, File/Directory Management, System Administration/Configuration, and Networking and Security.
* Hands on training in discovery and counter-infiltration methodologies.
* Proficient in Peripheral Security, Ports and protocols, Remote access security, and Wireless security.

**Cloud Infrastructure Architect/ Cyber Security Engineer**

**Paramount Solutions**, **CYBERCOE G6, Fort Gordon Georgia 30905 Sep 2013 to May 2014**

* Provided technical leadership to both the Systems Infrastructure and the Network Infrastructure teams.
* Implemented network security plan for the Cyber Campus Network (DC3T).
* Conducted CND network traffic analysis using various network monitoring tools.
* Experience on vulnerability assessment and penetration testing using various tools like Burpsuite, OWASP ZAP Proxy, NMap, SQLmap, Security Onion, Nessus, Kali Linux, and Metasploit.
* Creating and updating current signal training network IA policies and procedures.
* Conducting capabilities analysis, mission analysis, cost analysis and timeline planning.
* Developed CYBERCOE G6 Strategic Plan of Action on the Cyber Campus Network (DC3T).
* Network Data Center installation, configuration, maintenance, security, and backup and restore.
* Conducted risk management SDLC planning, and disaster recovery planning.
* Coordinating a Fort Gordon wide wireless network installation project.
* Creating the SOP and CONOP for the Cyber Campus Network (DC3T).
* Conducted weekly staff meetings and directed team development.
* Planning the redesign of the current Fort Gordon installation Datacenter and network architecture
* Operational planning and development of Cyber Campus Network (DC3T).
* Managed IT Infrastructure and any processes related to the systems.
* Implemented VMware cloud technologies in both a Windows and Linux environment.
* Implemented VMware’s ESXI, VSphere, Vcenter, VSAN, VRealize, and NSX technologies.
* Working Hands on Knowledge Installing and Deploying VMware ESXI virtual servers, Vsphere, Vcenter, Vshield, Vcloud Director, and ESXI host.

**Network Manager**

**NOVA-DINE Corporation**, **7th Cyber Mission Unit, Fort Gordon Georgia 30905 May 2011 to Sep 2013.**

* Hired, managed and trained two network division teams consisting of 15+ network team members.
* Managed over 150 Servers and up to 2000 users globally.
* Managed the fielding of CENTRIXS-ISAF for 44 deploying units in support of US Central Command into Afghanistan; supervised and validated IA packages and movements for CONUS transition of Brigade Combat Teams in to Theater.
* Proactively managed system development, implementation, integration, risk management, change management and contingency planning.
* Developed processes and Techniques, Tactics, and Procedures (TTP’s) on equipment, security procedures, personnel requirements and various other methods of documentation for company improvement.
* Implemented DISA STIGs on all of the networking equipment to maintain DISA STIGs compliance.
* Coordinated Configuration Control Board (CCB), Technical Reviews Board (TRB), and Technical working Group (TWG) meetings.
* Led two army network DIACAP accreditations which resulted in both networks becoming accredited.
* Conducted network vulnerability scans, Network Infrastructure Penetration Testing, and network security firewall and IDS rules.

**Senior Network Engineer**

**NOVA-DINE Corporation, 7th Cyber Mission Unit, Fort Gordon Georgia 30905**

**Dec 2010 to May 2011**

* As Subject Matter Expert ensured enterprise security concepts were implemented into the system network design, securely configuring systems and networks, validating and verifying integration of security onto systems, and ensured configuration management program was in place that recognized security.
* Maintained DIACAP compliance for Information Assurance and Vulnerability Assessment, hot fixes, and patches.
* Performed Cisco router, ASA firewall ACL, switch, and CUCM engineering, configuration and installed, configured and maintained TACACS+, VPN and GRE tunnels.
* Designed and implemented network diagrams of remote sites for visual presentations using Microsoft Visio 2010.
* Administered CA Spectrum, eHealth, and Solarwinds network monitoring tools and utilized Wireshark packet inspection tool.
* Performed Operations and Maintenance, and track IP, VLAN, and BGP community allocations on the CX-I CONUS network and the SIPR APC network.

**Systems Administrator**

**General Dynamics, NSA Fort Gordon, Georgia 30905** **Nov 2008 to Nov 2010**.

* Maintained Active Directory to include but not limited to the ability to create, delete and modify user and computer accounts, PKI, security and distribution groups, OU's and GPO's..
* Provided laptop, desktop, and enterprise datacenter server support including, Windows XP/Vista/7/UNIX support, network configuration, application configuration, user setup, Active Directory account creation, NETAPPS and hardware troubleshooting.
* Working knowledge with operating systems of Windows 2000/XP/Vista/7/UNIX/LINUX and server operating systems of Windows Server 2000/2003/2008 SQL and SharePoint.
* E-mail, server, network, and desktop support to staff of 400+ users locally.
* Directly interacted with customers and provided immediate troubleshooting in a fast paced and operationally critical environment.

**25B - Information Systems Operator/Analyst**

**US Army, 5th Special Forces Group, Fort Campbell, Kentucky 42223 Oct 2002 to Oct 2008.**

* As Subject Matter Expert oversaw and evaluated system security and backup procedures. Advocated, educated and enforced all internal and external security and privacy policies.
* Responsible for providing Technical and Project Management Leadership to multiple project teams of up to 100 people.
* Proficient in network and security technologies such as Firewalls, TCP/IP, LAN/WAN, IDS/IPS, Routing and Switching.
* Involved in planning and implementing future IT developments and project work as well as operational security
* Experience with VMware ESX administration and Virtual Machine operation.

**EDUCATION**

BS: Information Technology/Cybersecurity, SNHU, Projected Graduation Aug 2018

U.S. Army Signal School, Fort Gordon, GA

56 hours SANS Hacker Techniques, Exploits & Incident Handling course, Fort Gordon, GA

56 hours Computer Network Exploitation Boot camp, Fort Gordon, GA

40 hours CECOM TSD Network concepts course, Fort Gordon, GA

40 hours CECOM TSD OS Primer Course, Fort Gordon, Ga

40 hours CECOM TSD ADV Network Security concepts course, Fort Gordon, GA

40 hours CECOM TSD Security Concepts, Fort Gordon, GA

40 hours Malicious Network Analyst, Fort Gordon, GA

40 hours CECOM TSD Network concepts, Fort Gordon, GA

40 hours Malicious Network Analyst, Fort Gordon, GA

40 hours CNO Attack and Defend, Fort Gordon, GA

40 hours Cyber Threats Detection & Mitigation, Fort Gordon, GA

40 hours CNO Capabilities Developer’s Course, Fort Gordon, GA

40 hours Certified Ethical Hacker (C|EH) / EC-Council training course, Fort Gordon, Ga

40 hours of PMI project management Professional (PMP) education, Columbia, SC

**TECHNICAL EXPERTISE**

Red Hat Linux, Remote and Telecommuting, Python, UNIX, Linux (Kali, Ubuntu,) Microsoft Windows, SQL Server 2008, Exchange, Active Directory, Network Protocols: SSH, VPN, SIP, RTP, QOS, H323, MGCP, Citrix, Spectrum, Solarwinds, AWS, Azure, Google Cloud,(GCP, VMware ESXI, VMware Vcenter, VMware Vshield, VMware Cloud Director, DNS, TACACS, Nessus, Retina, Nexpose, NMAP, Wire Shark, Snort, PowerShell, Python, VoIP, Cisco ASA Firewalls, Palo Alto Firewalls, Security Onion, Voice Gateways, IDS, IPS, VPN, Authentication, CyberArk, Wireless security, Network Switches, routers, SAN, NETAPPS, SATCOM, ForeScout CounterAct, Network Analysis Tools (protocol analyzers), Red Team Methodologies, Blue Tem Methodologies, Physical Security, Information Security, Regulatory Compliance, Risk Assessments, Advising software and application development teams on data security, IT Management Systems, FEDRAMP, DoD Instruction 8500.01, 8520.2, DoD, DISA, and NSA Information Assurance Policy, Public Key Infrastructure (PKI), Department of Defense Directive (DoDD) 8500.1