Sr. Infrastructure Security Engineer Sr. Infrastructure Security Engineer Senior Infrastructure & Security Engineer Marlton, NJ Accomplished IT professional with an extensive background in systems engineering and cybersecurity. Experience in scalable and high availability datacenter design, Windows and Linux administration, networking, security architecture, IT governance, SOX/HIPAA/PCI DSS compliance, risk management, and disaster recovery and business continuity in financial and healthcare environments. Highly motivated, goal-oriented self-starter with a strong work ethic for team and individual projects. Authorized to work in the US for any employer Work Experience Sr. Infrastructure Security Engineer Capcare July 2015 to Present Designed and managed a hybrid infrastructure of both Azure cloud components and VMware, and Hyper-V clusters across multiple physical sites for scalability and to ensure business continuity. Leveraged technical information from threat feeds, intrusion detection alerts, firewall events, system and application logs, full packet captures, and endpoint process tracking to identify potential incidents, determine the root cause, and ensure the proper attack vector was mitigated. Managed CI/CD pipelines with Jenkins and Ansible and worked closely with development, infrastructure, and security teams on task automation and orchestration. Maintained a layered approach to network security consisting of firewalls, IDS/IPS, data encryption at rest and in transit, DLP, patch management, antivirus, SIEM, authentication and authorization, backup, and vulnerability assessments to identify threats and implement controls. Developed disaster recovery and business continuity plans for each site and implemented a new Veeam Backup & Replication infrastructure with local and offsite backup repositories and real-time replication to Azure with frequent automated backup recovery and integrity testing. Coordinated with management and stakeholders of business units to routinely conduct security audits, risk assessments, mitigate risks, and develop, implement, and perform tests of incident response and disaster recovery plans to ensure business continuity. Enforced compliance with HIPAA, PCI DSS, and SOX regulatory requirements to protect sensitive client information and intellectual property by implementing information security policies, centralized auditing, encryption, SIEM, secure file sharing, and data loss prevention solutions. Ensured all employees within business units were aware of compliance requirements and prepared for

assessments based on their respective role in information security. Engaged in continuous communication with management and stakeholders to discuss, research, and implement solutions to align with the evolving strategic initiatives of the business. Planned and managed Active Directory infrastructure including sites, organizational units, Group Policies, security groups, network access controls, and Azure AD Connect. Consolidated identity providers into Azure AD to automatically provision and secure applications, utilizing conditional access policies for multifactor authentication and SSO passthrough authentication for trusted domain-joined or Intune-managed devices. Designed cost-effective multi-petabyte, scalable, fault tolerant Ceph and Gluster storage clusters. Migrated Exchange mailboxes to Office 365 with Advanced Threat Protection and Mimecast for archiving and to defend against malicious attachments, spam, and phishing attacks. Performed live migrations of on-prem and AWS virtual machines, applications, and SQL databases to Azure using Express Route with no downtime or loss of data. Cybersecurity Analyst Captive Planning Associates August 2013 to July 2015 Performed technical investigations of potential internal and external threats to information assets. Performed malware analysis and forensic examinations to find malicious patterns and origin. Utilized security tools including endpoint security, SIEM, DLP, IRM, vulnerability assessment utilities, and patch management. Monitored, triaged, analyzed, and responded to security events in real-time, providing real time analysis of potential attacks and root cause analysis. Baselined and normalized environments to better identify anomalous activity. Advised on specific defensive actions to take and identified additional indicators of compromise during investigation phases. Documented and tracked in detail all aspects of cybersecurity investigations to resolution and gathered evidence of security breaches to assist law enforcement when necessary. Interfaced with management directly and provided guidance during incident response efforts. Assisted with the maintenance of actionable intelligence based on current threats and trends. Provided support to the assessment team with vulnerability scanning and assisted in remediation. Created a security architecture of policies and standard operating processes and procedures. Provided security awareness and training programs for employees. IT Consultant AutopilIT 2009 to August 2013 Worked as an independent consultant, providing IT

solutions & support for local small businesses in healthcare and finance industries. Provided troubleshooting assistance for a variety of industry-specific applications. Restructured and upgraded customer environments that had been implemented and abandoned. Worked within strict budget and time constraints, with minimal disruptions to business. Migrated clients legacy PSTN phone services to cloud-based IP phone systems. Implemented Twilio Elastic SIP Trunking and OpenSIPS as a SIP proxy for NAT traversal. Organized efforts to upgrade all workstations to customized Windows images, deployed and managed with ManageEngine Desktop Central. Implemented site-to-site VPN tunnels using OpenVPN and L2TP/IPSec between offices. Implemented DirectAccess always-on SSL VPN for remote access from laptops. Implemented a remote access infrastructure using Remote Desktop VDI and XenDesktop with Duo Security multifactor authentication. Education Bachelor's in Computing & Security Technology (4.0 GPA) Drexel University - Philadelphia, PA 2009 to June 2013 Skills Computer Forensics (6 years), Project planning (7 years), VMware (7 years), Mcse, Linux (8 years), Microsoft Office (10+ years), Routing (10+ years), Veeam (5 years), GlusterFS (5 years), Ceph (5 years), Active Directory (10+ years), PKI (10+ years), Microsoft Azure (3 years), Google Cloud Platform (1 year), AWS (3 years), Sysinternals Suite, Web Development (10+ years), Risk Management (7 years), Wireless (8 years), Office 365 (5 years), Exchange Server (5 years), Citrix (4 years), Graylog (4 years), Project Management (7 years), 3CX (2 years), PBX (4 years), Twilio (4 years), Nessus (7 years), Bit9 Carbon Black (3 years), Software defined storage (6 years), Hyper-V (3 years), Dell (7 years), EMC (5 years), Disaster Recovery (7 years), Business Continuity (7 years), VMware vSphere (6 years), Windows Server (10+ years), CentOS (7 years), Dell EMC (7 years), Group Policy (7 years), OpenVPN (8 years), DLP (6 years), Data Loss Prevention (6 years), VPN (8 years), Firewalls (8 years), VLANs (7 years), Forward and reverse proxies (5 years), WSUS (6 years), Auditing (7 years), DNS (10+ years), Docker (3 years), VDI (7 years), Citrix Xenapp (4 years), Citrix XenDesktop (4 years), RemoteApp (7 years), Checkpoint (3 years), Splunk (5 years), Sourcefire (5 years), PowerShell (5 years), Python (5 years), git (5 years), Apache (8 years), nginx (8 years), PostgresSQL (5 years), MySQL (8 years), Load balancing (8 years), HAproxy (8 years), IIS (5

years), Snort (5 years), McAfee ePO (5 years), pfSense (10+ years), Memcached (6 years), Networking (10+ years), AccessData Forensic Toolkit (5 years), HTTP (10+ years), HTTPS (10+ years), FTP (10+ years), SSH (10+ years), DNS (10+ years), SSL (10+ years), DHCP (10+ years), Switching (10+ years), Subnetting (10+ years), DevOps (5 years) Certifications/Licenses VMware Certified Professional Data Center Virtualization 6.5 2015 to Present AccessData Certified Examiner 2013 Network+ 2011 CIW Web Foundations Associate 2011 VCP5-DCV 2015 Additional Information Skills: Project planning and management, computer forensics, web development, risk management

Name: Michael Branch

Email: jennifer68@example.net

Phone: (516)259-1728x1931