Sr. Security Engineer for IT Security Sr. Security Engineer for IT Security Sr. Security Engineer for IT Security - AIR MEDICAL GROUP HOLDINGS San Diego, CA Over 18 years of professional experience in Information Security, including but not limited to: Identity and Access Management, Vulnerability Management, PCI Compliance, Audit, eDiscovery, Digital Forensics, and HR / Corporate Security Employee Investigations. Bachelor of Science in 'Organizational Security and Management/Criminal Justice' (with Honors). Currently holds the following certifications: CISSP (Information Systems Security Professional); CIAM (Certified Identity and Access Manager); CHFI (Computer Hacking Forensic Investigator); Qualys Certified Specialist (VM, and PCI); DBA OCA 10g; Security+, and ITIL Foundation. Member of: 'The National Criminal Justice Honor Society', and 'Identity Management Institute, Center for Identity Governance'. Highly driven self-starter with a strong work ethic; received several project and performance based awards. Work Experience Sr. Security Engineer for IT Security AIR MEDICAL GROUP HOLDINGS - San Diego, CA January 2019 to Present Contract via Matrix) Systems Administration and Vulnerability Management Administration tasks of MFA using DUO, and also OKTA. Responsible for vulnerability scanning and reporting using Nessus/Tenable.sc Maintain and report compliance/scan through Elavon's PCI Compliance Mgr. Creation of web application scans using AppSpider/Rapid7 and Nessus/Tenable.io Performs web content control; reporting; and scanning of infected endpoints via Bitdefender Gravityzone. Utilizes Absolute 7.4 in order locate a stolen or missing device, and to freeze (brick) a device as needed. Uses ZIX Email Threat Protection solution to whitelist/blacklist; report spam; and review quarantined emails. Allgress 6.x GRC platform administrator. Use of Netwrix Auditor for research and reporting. Process IT Security related requests; schedule Change Management via ServiceNow. Office365 environment; Maintain Security board in Planview LeanKit; Provides metrics. IT Security Specialist III for Global Technology and Operations BANK OF AMERICA - Addison, TX July 2018 to December 2018 Contract via TEKsystems) Identity and Access Management Process Identity and Access Management requests received via ARM (Access Request Manager). Provision and maintain access (Grant/Modify/Delete) with a focus on 'Retail and Preferred' applications, including but not

limited to: DWAC (Deposit/Withdrawal at Custodian); Document Mgmt. Portal; Thomson Reuters Deal Tracker; RPM-AS400; LexisNexis; CS_ Security (Card Services); FlashWeb; Merlin Teller; CheckFree PartnerCare; Genesis Biller; and COMPASS Access Mgmt. (CASHEDGE) by fiserv. Review Profile Templates to ensure least privilege is requested and granted. Utilize QWS3270 Secure v4.8 to access CSDB to verify employment status/other pertinent Associate information. Sr. Information Security Analyst AMERICAN AIRLINES - Fort Worth, TX March 2015 to July 2018 for Cyber Security Operations Center Vulnerability Management and Compliance Administration, scanning, reporting, and lifecycle management of Qualys for two legacy airlines (American Airlines & US Airways) as the result of a merger. Maintain and report compliance/scan through Qualys PCI. Supported yearly PCI assessment on behalf of Vulnerability Mgmt. Program by working with 3rd party vendor(s) in support of PCI DSS compliance. Provided Brinqa Vulnerability Management Platform administration. Used OIM (Oracle Identity Manager) to maintain Qualys service account, and perform other user functions. Assessed/proof of concept of possible replacement tools. Use of RSA Archer eGRC to maintain DR (disaster recovery) docs, and identify application owners. Incorporated the Agile methodology through the use of Rally for projects. BMC Service Desk Express and ServiceNow used for Change Management and Ticketing. Received multiple 'Above & Beyond' awards for my accomplishments with Qualys / vulnerability management program. Sr. Information Response Analyst for Information Security AMERICAN AIRLINES - Fort Worth, TX September 2012 to March 2015 e-Discovery/Digital Forensics/Employee Investigations Performed evidence gathering for Employee investigations, as a technical contact for HR/Corporate Security. This included anything from time card fraud, PII (personally identifiable information), to performing Computer Forensics for possible pornography, using AccessData FTK 1.81.6 and AccessData FTK 3.4. Collected computer images for Legal cases, using AccessData FTK Imager 3.1.1.8. Performed mobile device collections, using Cellebrite, as part of eDiscovery data gathering for Legal cases. Assisted in the collection and documenting of ESI (electronically stored information), by using various tools to collect Email PSTs (Clearwell), Home Directories, Shared Directories (Pinpoint SafeCopy), and archive email (LiveOffice and Enterprise Vault). Used IBM PSS Atlas and Exterro

Fusion (Case Management Software for Legal Matters and collection tracking) Administration of Symantec Clearwell 7.1.2; setting up case reviewers, archiving cases, pulling email PST's and related. Maintained a Forensic lab. Assisted Desktop Svcs with data retrieval and recovery issues as needed. Used various additional tools/applications, such as: Image Masster - Solo III Forensics (duplicate / wipe drives); Tableau Write Blocker (view drive with write protection);; X1 Social Discovery (crawl and/or capture web content); Highest collection success rate. Sr. Information Security Analyst for IT Security AMERICAN AIRLINES - Fort Worth, TX February 2010 to September 2012 Contract via TEKsystems) Incident Response and Employee Investigations IBM QRadar SIEM 7.1 administrator. Worked with Engineer of Managed Services, assisting with verifying log ingestion, setting policies such as data retention, and working with our internal IT Audit in reviewing licensing, configurations, and providing supporting documentation toward audit. Performed evidence gathering for Employee investigations, as a technical contact for HR/Corporate Security. IBM Security QRadar SIEM 7.1 (log mgmt. tool used for Investigations); McAfee Web Reporter Version 5.2.0.06 (Internet browsing reports); RSA Archer eGRC v 5 (Investigations tracking), and Active Directory. Used SAM (System Access Manager), having administrative duties over various tasks. Participated in the pilot group toward selecting possible replacement for Websense Enterprise Reporting v6.3. Served as an escalation contact for Tier 4 Network group for network utilization issues as the result of Internet downloads and related usage. Created reporting and processes surrounding rogue wireless devices from Cisco WCS to satisfy audit requirements for Mobility team. Received an 'HR Partnership Award' Sr. Analyst for Technology Infrastructure CITIGROUP - Irving, TX June 2009 to February 2010 Database Analyst Responsible for gathering requirements from the business for new reports and tool functionality toward the conversion automation tool, as part of the Desktop Standardization Initiative. Create and update documentation and reports to be posted on Sharepoint, with functions as a SharePoint owner. Work closely with developers to resolve findings and recommend improvements, and perform testing before moving any changes to production. Reviewed/updated policy information in RSA Archer. Utilized MS Access, SQL, MS Office 2007, and SharePoint for reporting. Used Planview

Enterprise 9.0.1 for projects and time keeping. Used Thin Client office connectivity and Citrix remote access. Trained other contract staff. Security Architect GMAC ResCap/Mortgage - Lewisville, TX March 2008 to January 2009 for Security Group IBM/ISS Site Protector Administrator Performed monitoring and analysis of IDS/IPS via IBM/ISS Site Protector. Migrated two sites into one - IBM/ISS Site Protector Documents, reports, researches issues and tracks remediation progress. Responsible for updates, configuring alert responses, and policy updates. Created how-to documentation for IDS/IPS tasks. Researches and reports on existing and emerging technologies and vulnerabilities. Evaluates IDS/IPS products. Evaluated, and ultimately provided support and administration of NetIQ Security Manager on behalf of another team, due to my Access Management background. Utilized other tools and applications such as RSA enVision, Provider-1/CheckPoint, and Clarity for project tracking and time reporting. Utilized Altiris for asset research. Used MS SQL Server queries. Network Security Analyst for Network Team AMERICREDIT CORP - Arlington, TX April 2007 to March 2008 Vulnerability Management Performed Websense 6.3 Internet content filtering administration and reporting (Reporter and Manager), as well as, provide Internet reporting to HR for Employee Investigations. Initiated, coordinated, and participated in Websense cleanup project using Active Directory groups vs. by user acct. Performed internal vulnerability scans using eEye Retina, McAfee Foundstone 5.0, and Nessus scanners, while tracking issues and remediation progress. Performed database scans using AppDetectivePro. Created 'how to' documentation for common tasks for cross-training of staff. Generated Bindview and Configuresoft Enterprise Configuration Manager reporting. Maintain licensing, as well as Entrust certificate information for company. Create and maintain MS Access databases within dept, including Risk Assessment database. Performed SQL reporting and reconciliation functions. Maintenance of IDS via ISS Site Protector. Department contact for all Audit related inquiries Incidents tracked via Magic and Remedy ticketing systems. Sr. Application Security Analyst for IT Applications Team AMERICREDIT CORP - Arlington, TX March 2005 to April 2007 Identity and Access Management Responsible for granting, maintaining access for the Enterprise based on need-to-know need-to-do basis by demonstrating experience implementing

platform-specific authentication and authorization services on: Microsoft Active Directory, AS/400, CACS, Oracle Products, UNIX, Mainframe/RACF and Cognos. Reconciled HR onboarding/off boarding against access requests via Cognos reporting. Performed Win-Pak 2.0 Release 3 badge administration (user/template administration, reporting and reconciliation). Performed yearly financial apps. re-certification (AS400, CACS, Oracle Data Warehouse and Oracle ERP) in conjunction with 3rd party audit. Provisioned 3rd party applications including, but not limited to: LexisNexis, Salesforce and Deal Tracker (where I was one of only 3 people in the company who administered eVault access). Created templates for company job titles, as well as maintaining a template database with network access requirements and badge access requirements identified by job title. Worked with other technical groups and developers to have tasks streamlined and to give recommendations for process and tool modifications. Department contact for all Audit related inquiries Audit the work of junior analysts. Generate Remedy stats via Crystal Reports. EDI Data Analyst for EDI Data Management CAPGEMINI ENERGY - Dallas, TX October 2003 to February 2005 Electronic Data Interchange Responsible for analyzing, resolving and reconciling Electronic Data Interchange (EDI) transaction data into/out of Revenue Systems. Used SQL queries, EDISIM 5.0, Excel, Golden 32 5.7, UltraEdit during analysis to pull data from Oracle tables and QWS3270 to pull data from DB2 tables to identify business data and quality issues. (Researched and resolved 2-year backlog of error transactions. Trained senior team members and management on issues and resolution). Ensured completion/delivery of Electronic Data Interchange (EDI) transactions based on market rules, protocols and tariffs to market participants and Electric Reliability Council of Texas (ERCOT). Identified system defects and tool development needs. Worked with developers to automate repetitive tasks, have templates created, and gave feedback on tool modifications. Sr. Data Security Analyst for Information Security BANK OF AMERICA - Dallas, TX January 1999 to July 2003 Identity and Access Management Responsible for analyzing and resolving security issues and daily access administration at the object level in accordance with Identity and Access Management policies and procedures. Created user ids and verified employee data in the Mainframe via TSO. Provided Microsoft NT 4.0, Windows 2000 (Active Directory) and Novell

Netware 3.X system administration nationwide with emphasis on security and access control. Responsible for account/group moves, adds and deletes, as well as coordinating data moves and migrations as part of consolidation from NationsBank merger. Monitored work queue and had assignment responsibilities as backup to Team Manager. Served as subject matter expert by being the 'Exceptions' contact for the department. Performed server clean-up activities, standardizing user ids on Novell server installs. Received several project and performance based awards: 'Leadership', 'Trusting and Teamwork' and 'Doing the Right Thing'. Used the following additional applications/platforms: Lotus Notes 5 & 4.5, Extra! 4.2 (Mainframe), Microsoft Applications on 2 Compaq Deskpro Pentium II's (one with Windows NT Workstation and the other with Windows 2000 Workstation) and an IBM ThinkPad Laptop with dual boot (Windows NT and Windows 2000). Dial-in via PC Anywhere, Hard Token and Soft Token. Network Administrator ARTHUR ANDERSEN - Miami, FL September 1998 to January 1999 South Florida for Tax and Audit Novell Administrator for Miami, Ft. Lauderdale, and West Palm Beach offices. Lead Network Analyst for Global Network Operations Center ANDERSEN CONSULTING - Dallas, TX January 1996 to September 1998 Network Operations Education Bachelor's Skills Cyber Security, Information Security

Name: Martin Bennett

Email: hodgeallison@example.net

Phone: 001-634-593-0720x296