MIKE T BAILEY

IT/Security Professional

E-MAIL: ITPRO@MIKETBAILEY.COM
PHONE: (913) 259-4682
HOMETOWN: OVERLAND PARK, KS
WEBSITE: WWW.MIKETBAILEY.COM

Multi-certified technology professional who has been working in the Information Technology field since 1993. Qualifications include a BS degree in Telecommunications Management; knowledge of Information Security, Information Technology and a business acumen to enforce various levels of confidentiality, integrity and availability.

- Solid knowledge of LAN/WAN network administration and support under Microsoft Windowsenvironments.
- Secure business assets using proven internal security standards.
- Securing operating systems, networks, and applications from attacks utilizing patch and vulnerability management
- Experience with Active Directory and group policies in Windows 2000 – Windows 2008R2
- Experience using SQL Server Management Studio to run queries in both SQL Server 2005 and SQL Server 2008.
- Proven expertise in supporting and troubleshootinghardware, software and networking issues.
- Organized, take-charge professional with exceptional follow-through abilities and detail orientation, able to plan and oversee projects from conception to successful conclusions.
- Some exposure to Linux OS's: CentOS, Redhat, and Ubuntu.
- Outstanding communication skills; interfaces effectively with upper management, vendors, staff, peers and users.
- Business acumen / Contract negotiations / Project Management
- Continually striving for additional educational and learning opportunities.

CERTIFICATIONS

Security+•LogRhythmCertified Professional •Blue Coat Certified Proxy Professional (BCCPP)
Blue Coat Certified Proxy Administrator (BCCPA)•ITIL v.2011 Foundation
Sourcefire Certified Professional (SFCP)•Certified Virtualization Expert 4.1 • Network+ • I-Net+ • CIW Associate

TECHNICAL SKILLS

Hardware:	Servers, Desktops, Laptops, Printers, Switches, Syspine and 3Com IP phone systems,
Systems:	MS Windows Server 2000/2003/2008R2/2012/Small Business Server 2008/2011, Mac OS, MS Exchange 2000/2003/2007/2010, MS Windows 95/98/XP/7/8, Some exposure to Linux OS's: CentOS, Redhat, and Ubuntu, VMware vSphere, VMware Workstation, MS Hyper-V
Networking:	Active Directory, TCP/IP, DNS, DHCP, Voice/Data Cabling
Software:	Symantec Ghost,Veritas Backup Exec, CA ARCserve,ShadowProtect, MS Office SuiteXP-Current, Microsoft FrontPage, Adobe Dreamweaver, Adobe Fireworks, Adobe Photoshop, ConnectWise, LabTech
Security	LogRhythm SIEM, Checkpoint Firewall, Bluecoat Proxy, Sourcefire IPS, McAfee SIEM, Sourcefire Firewall, SonicWall 3500 Firewalls, SonicWall 2500 VPNs, Symantec AntiVirus, Symantec Endpoint Security, Symantec Mail Security, CyBlock Filtering Proxy Server, Routers

EDUCATION

Computer Hacking Forensic Investigator January 2014	LogRhythm SIEM November 2013	Linux October 2013
Check Point September 2013	Bluecoat August 2013	Sourcefire July 2013
CEH v7 (Certified Ethical Hacker) May 2013	CISSP April 2013	ITIL v.2011 Foundation April 2013
VMware Infrastructure vSphere 4.1 January 2011	SCNP Network Defense and Countermeasures October 2002	SCNP Network Security Fundamentals September 2002
Microsoft Networking Professional Diploma National American University, Kansas City, Missouri May 2002	BS Degree, Telecommunications Management DeVry Institute of Technology, Kansas City, Missouri February 1993	

WORK EXPERIENCE

Network Security Engineer - Axelacare . . . . . May '15 – Present
Developed and implemented the company's computer security incident response plan based on NIST standards (SP 800-61, SP 800-66) to meet HIPAA compliance guidelines. Developed and implemented security standards, guidelines, and procedures. Conduct monthly health checking of all Company network infrastructure and systems to ensure compliance with the company'ssecurity policy and contractual obligations and document results. Setup and configured Solarwinds LEM (SIEM) product to monitor logs from various servers and to alert on security incidents. Own the immediate containment and investigation of any security incidents to the company's network devices, systems, storage, and company/customer proprietary information. Work with third party managed security services vendor on resolving any security incidents. Update the Barracuda web filters blocked list(s) with rogue and/or threatening IP addresses and URLs when necessary. Review Watchguard firewall logs and update policies when necessary. Setup and configured Solarwinds Orion product to monitor health and connectivity of enterprise devices. Run vulnerability scans using OpenVAS installed on Kali Linux virtual machine against internal networks and provide results to management and other IT members. Serve as primary point of contact for external third party security audits. Created network diagrams of the MPLS connectivity between remote sites and equipment rack diagrams in both data center locations.

Security Engineer - Foresite. . . . . April '14 – May '15
Provide remote security device management and support. Implement access control and security policy per requests and providing level 3 support to the Security Analysts. Support monitoring real-time event data, keeping abreast of intelligence from the IT security community and government/law-enforcement, or other industry sources. Implement change requests and provide 3rd level troubleshooting support. Analyze security event data from various computing platforms, network elements, and security devices. Perform system/network inventory, configuration management, operational ticket submission, request tracking, and problem resolution. Active system tuning for short term rules (i.e. temporary suppression) and approval of new rule logic for implementation. Design and document new MSSP client deliverables for onboarding. Develop, document, and maintain operational processes and training documentation. Lead incident response calls and interface with customer during incidents. Collect, Consolidate, & Communicate weekly activity reports and performance metrics to leadership.

MSS Security Analyst – Fishnet Security. . . . . .June ‘13 – March '14
Provide security monitoring, event analysis and countermeasure proposals in Information Technology Security on behalf of clients to reduce the impact of security incidents and system compromises. Analyze and respond to security threats and configuration issues from Firewall (FW), Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), Antivirus (AV), Network Access Control (NAC) and other client data sources. Perform network troubleshooting to isolate and diagnose common network problems. Train new Security Analysts on the use of LogRhythm SIEM and how to differentiate between real and false security threats. Provide guidance to new Security Analysts on researching security threats and the proper way to report those threats to the clients.

Systems/Network Administrator – Jack Henry & Associates. . . . . July ‘10 – Jan '13
Responsible for monitoring, modifying and maintaining systems in a load balanced, multi-data center environment for confidentiality, integrity, and availability to customers. Part of a team in charge of the deployment and hosting of 20+ products that service total transaction volumes of over $40 million a day. Systems include, but are not limited to, data center, network, operating system, product development, mail server, applications server and groupware. Implement system enhancements to improve the performance and reliability of the system. Build, configure, and install servers in a VMware ESXi environment. Coordinated with various groups to schedule downtimes/maintenance events. Administer Windows Server 2003 and 2008 based systems. Troubleshoot and resolve customer and internally-reported system problems received from the internal ticketing system. Document and implement system procedures, policies and events. Perform essential functions required for effective system backup, including management of onsite/offsite backup tapes, using CA ARCserve software and IBM TS3310 tape library. Configuration of existing and new monitors within DeepMetrixipMonitor 6.1. Use F5 Big-IP configuration utility to manage the network between data centers. Managed more than 700 DNS domain names for external clients using F5 Networks’ BigIP-1600 Global Traffic Manager (GTM) devices. Exposure to IIS 6.0 and IIS 7.0 website administration. Exposure to CiscoView device manager and Cisco Application Networking Manager to manage server availability at corresponding data centers. Managed the new installation of Cisco Application Networking Manager virtual appliance to replace the old system running on a RedHat machine. Use SQL Server Management Studio 2008 to run queries and create reports with the data pulled from the SQL database. Assist other groups with file management using FTP and within AIX 5 (file upload, file permissions and file ownership).

Network Administrator – CTSS, Inc. . . . . March '08 – July '10
Responsible for the hardware, software, networks and security of CTSS clients' Information Technology infrastructure. The main clients included: Headache and Pain Center, Doctors Specialty Hospital, Weight Loss Surgical Center, and Nemechek Health Renewal. Services include but not limited to the administrationof Microsoft Windows servers, Microsoft Exchange (2003/2007), Active Directory domains, CyBlock Filtering Proxy Server, Syspine IP phone system, and 3Com NBX V5000 IP phone system. Configuration, installation, and troubleshooting of Dell switches. Troubleshootingof existing and installation of new voice cabling, including 66 and 110 punch blocks and corresponding cross-connects. Configuration and maintenance of network security appliances (SonicWall Firewalls, Symantec Endpoint Security, and Symantec Mail Security for Microsoft Exchange). Performing routine audits of Windows 2000 through 2008 Servers and 3rd party medical practice, back office software. Configuration and maintenance of Microsoft Windows servers, desktops and peripherals. Maintain proper security access control for file and print shares. Maintain proper access to various components within GE Centricity® practice management software. General administration of Healthland Physician Practice Management system installed on IBM AIX Unix server including but not limited to settingup new users, password resets, and monitoring print queues. Monitor and maintain daily backup tapes using Veritas Backup Exec. Worked with third party audit company to reviewand certifyall back-up and disaster recovery procedures
maintainedcompliance with necessary HIPPA guidelinesand regulations. Other duties include supporting and troubleshooting a variety of daily end user problems. Deployment of software patches/upgrades and configuration changes utilizing WSUS.. Creating and restoring desktop images utilizing Symantec Ghost 11. Utilize remote connectivity software such as Microsoft Remote Desktop and Tight VNC to remotely troubleshootissues.Effective oral and written communication with various levels of management providing consultation and expert advice on systems related topics. Setup CTSS help desk website utilizing Joomla with integrationof osTicket. Setup VLAN for test environment at main CTSS office location. Install, setup and test Virtual Iron server virtualization & virtual infrastructure management solution.Maintain an accurate record of hours spent on Work Orders and projects. Maintain a moderate and increasing level of proficiency in hardware, software, and other technologies supported by CTSS. Managed less experienced technical staff at Headache and Pain Center. Used leadership skills to influence and counsel less experienced technical staff. Create and/or update documentationusing Microsoft Word and/or Excel to benefit other IT personnel.

Production Support Technical Analyst – Federal Reserve Bank. . . . . Feb '06 – April '07
Provide support to all Federal Reserve System check-processing sites to resolve complex problems associated with all aspects of check processing in a time-critical, deadline-driven environment. Proactively monitor systems using various software tools for early problem detection and ensure processing remains on schedule for each of the 32 offices nationwide. Perform process improvement initiatives that affect the standard check environment, as well as develop and maintain departmental procedures and standards. Provide a calming influence on others in a crisis situation.

INDUSTRIES

Information Security, Financial, Manufacturing, Telecommunications, Retail, Legal, Utilities, Managed Services, Banking, Real Estate, Dental, Health Services