Information/Network Security Engineer

Josh Burke

(address/phone available on request via e-mail)
E-mail: resume-20080212@r20080212.tempmail.iokui.com

SUMMARY

Broad knowledge of hardware, software, and networking technologies to provide a powerful combination of analysis, implementation, and support. Experience in system and network administration and engineering, hardware evaluation, project management, systems and network security, incident analysis and recovery.

OBJECTIVE

Provide network, systems, and security experience, knowledge, and solutions in a system and network-diverse environment. Protect confidentiality, integrity, and availability of information and information systems. Advise and engineer secure solutions for business opportunities. Learn and experience, mentor and share.

EXPERIENCE

10/2005 – 09/2006   Getty Images   Seattle, WA
Information Security Analyst III

Provide technical leadership to the enterprise for the information security program. Mentor and train others in information security in addition to training for other technical groups. Install and maintain security infrastructure, including IPS, IDS, log management, and security assessment systems. Assess threats, risks, and vulnerabilities from emerging security issues. Publish Security Updates newsletter for technical groups. Draft enterprise security standards and guidelines for system configuration. Managed process and acted in the lead role for computer security incident response team. Perform and create procedures for system security audits, penetration-tests, and vulnerability assessments. Develop scripts to maintain and backup key security systems.

12/2004 – 10/2005   Starbucks Coffee Company   Seattle, WA
Information Security Analyst – Technical

Recommended preventive, mitigating, and compensating controls to ensure the appropriate level of protection and adherence to the goals of the overall information security strategy. Assisted in the development of access-controls, separation of duties, and roles. Conducted technical risk evaluation of hardware, software, and installed systems and networks. Assisted with testing of installed systems to ensure protection strategies are properly implemented and working as intended. Assisted in incident response and recommend corrective actions. Communicated with personnel about potential threats to the work environment. Participated in forensic recovery and analysis. Participated in development and maintenance of global information security policy.

11/2002 – 12/2004   BECU (formerly Boeing   Tukwila, WA
                      Employees Credit Union)
IT Network & Security Analyst

Maintained security of voice and data networks and equipment. Monitored and maintained physical and logical security and access to systems. Responsible for support of existing security policies and procedures, as well as creation and implementation of new security procedures. Risk assessment of partners. Presented options to management for the enhancement of DNS, firewall, modernization of firewalls, and inbound e-mail security and robustness. Assisted with the upkeep of network infrastructure including switches and load balancers. Assisted in migration of VPN concentrators to new project. Achievements include completing TruSecure enterprise certification, and development of incident handling procedures.

1/2001 - 8/2002   Internap Network Services   Seattle, WA
Security Systems Engineer, Core Systems Development

Used previous experience in company to focus on securing information and systems. Trained and mentored employees in many job descriptions regarding security and system basics, best practices, etc. Documented exiting and in-development policies, procedures, and systems. Deployed distributed intrusion detection sensor network. Security lead on new product design team. Business continuity consulting. Developed into lead security person at company.

12/1999 - 1/2001   Internap Network Services   Seattle, WA

Systems Engineer, Core Systems Development

Used knowledge of bind, apache, SSH, and security to retrofit existing systems and engineer new, improved security systems. Firewall creation and maintenance using Cisco ACL and Linux iptables. Basic Cisco 2900/5500 switch configuration and maintenance. Participated on Y2k rollover team, and on-call internal CERT team. Trained end-users on system architecture and use. Expanded documentation.

7/1998 - 12/1999   Internap Network Services   Seattle, WA

Systems Administrator, Core Systems Development

Participated in creation of Systems Operations Center for the company, which maintained hundreds of systems and applications spread throughout the world. Responsibilities included end-user troubleshooting, document creation, and system design. Acted as Intranet webmaster and helped create and administer security policies.

EDUCATION

12/2000   University of Washington   US-WA-Bothell

Bachelor's Degree

Bachelor of Arts in Business Administration. Emphasis in Technology and Innovation Management. Coursework in new product development, organizational management, international business.

AFFILIATIONS

9/1997 – Present   WCUG (Western Computer User Group)   Alumni Member, list moderator.

SKILLS

Skill Name	Skill Level	Experience
Unix – Linux System Administration (Debian/Red Hat)	Expert	7 years
IP Packet Analysis - Ethereal, tcpdump, ntop	Expert	6 years
Intrusion Detection - Snort/ACID, TippingPoint	Intermediate	4 years
Penetration Testing - Nessus/Nmap	Expert	5 years
DNS Administration (bind)	Expert	5 years
Perl, HTML	Intermediate	5 years
Apache, Asterisk, DHCP, Exim, Munin, MySQL, Postfix, SAMBA, SSH Administration	Expert	5 years
Cisco IOS Configuration (Netflow, ACLs, TAC+/Tacacs)	Intermediate	5 years
Citrix Metaframe Administration	Intermediate	4 years
Sidewinder/Gauntlet Firewall Administration	Intermediate	2 years
Sonicwall Firewall Administration	Intermediate	2 years
F5 BigIP and 3DNS Administration	Intermediate	3 years
Subversion Change Management Administration	Beginner	2 years
Nortel Contivity VPN Administration	Beginner	1 year
Unix - Solaris System Administration	Beginner	1 year
Cisco MARS Administration	Beginner	1 year

ADDITIONAL INFORMATION

CISSP - Certified Information Systems Security Professional for more than 3 years.

Previous projects: Co-author "Wireshark & Ethereal Network Protocol Analyzer Toolkit". Technical Editing: "Snort, Ethereal, and Nessus power tools" Syngress. "Red Hat: A Beginner's Guide" McGraw-Hill/Osborne.

References available upon request.