

Security Engineer Security Engineer Security Engineer Cincinnati, OH Authorized to work in the US for any employer Work Experience Security Engineer Encore Technologies - Cincinnati, OH May 2016 to March 2017 Contributed and participated in the build-out of the initial Security Program at Encore Technologies. Deployed, customized, and managed AlienVault System Information Event Management. It consisted of monitoring network and system events, along with alarms, vulnerability management and scans, asset management (over 500 machines), enterprise logging that derived from HIDS, Rsyslog, and/or specific application plugins, and reporting. This entailed heavy use of Linux OS, as well as Windows Server and Red Hat Enterprise. AlienVault was a customized version of Debian Linux, running a combination of MySQL, Apache2, and Python. Various software packages were included like OpenVAS, Nagios, OSSEC, Suricata, and nMap. Deployed, customized, and managed Enterprise Password Vault (Thycotic Secret Server) integrated with Duo Dual Factor Authentication. Password Vault was deployed on Windows Server 2012, and used SQL server on the backend with IIS as the Web Server. Incorporated over 35 users for centralized, secure password management. Provided some insight into necessary documentation such as policies (minimal), as well as documented numerous procedures for AlienVault, Thycotic, and Duo.

IT Business Controls/Risk Analyst Adecco - Cincinnati, OH January 2016 to May 2016 Fifth Third Bank Corp., Cincinnati, OH Assisted in leading risk management initiative to assess approximately 10,000 databases throughout the network with nearly 900 different users. Evaluated various elements of risk, including, but not limited to data classifications and recovery time objectives, to provide risk and criticality ratings. Ratings were used to classify files amongst different 'Tools' (Office Tool, User Tool, Managed Tool) which could then be further assessed and managed accordingly. Contributed to initial framework of IT Business Controls User Tool policy, and aided in the creation of the first revision. Participated in Outside Service Provider reviews which calculated different areas of risk encountered by the use of third-party vendors, services, and software. Security Researcher/Analyst University of Cincinnati - Cincinnati, OH May 2014 to May 2015 Extensively researched the different types of honeypots, their uses, and their importance in the security field. Created a high interaction honeypot deployment with the use of three separate machines running Linux exclusively.

Used a LAMP stack with LogAnalyzer to monitor logs from rsyslog for all the machines in the deployment. Once compromised, the deployment uses the SSH tunnel to monitor all keystrokes of the attacker and has playback functionality. Three instances have been deployed on UC's DMZ at a month's time and incurred over 11,000 login attempts from IP addresses all over the world. Research went on to be published in the Association of Computing Machinery. Technologies: Linux (CentOS, Debian, Deft, Fedora, IPCop, Kali, Knoppix, OpenFiler, pfSense (BSD), SecurityOnion, Tails, Ubuntu), Apache, CLI, Cron, LogAnalyzer, IPTables, MySQL, Metasploit, NMap, Nessus, OpenVPN, rsyslog, Samba, SSH, Wine, GNS3, ESXi, VMware vCloud, VMware Workstation, Vmotion, VirtualBox, Microsoft Windows (2000, XP, 7, Server 2003, Server 2008, Server 2012), Active Directory, IIS, iSCSI, RDP, Volunteer Experience & Participation Education Bachelor of Science in Information Technology in included University of Cincinnati - Cincinnati, OH High School Diploma Archbishop Moeller High School Certifications/Licenses CompTIA A+ August 2010 to Present CompTIA Network+ October 2010 to Present CompTIA Security+ December 2010 to Present CompTIA Linux+ August 2013 to August 2018

Name: Brittany Shaw

Email: carlbrown@example.net

Phone: 512.673.3490x62343