IT Security Analyst IT Security Analyst IT Security Analyst - Ashley Inc Bel Air, MD Authorized to work in the US for any employer Work Experience IT Security Analyst Ashley Inc - Havre de Grace, MD September 2015 to Present 1. OSINT familiar experience 2. Implemented and designed MFA projects to allow MFA throughout the organization to increase security accountability and authorization for all staff Designed and implemented SIEM solution to correlate logs from many high security systems and the like to a central location allowing for reporting and threat hunting. Implemented Network performance monitoring and solutions to monitor CPU RAM and connectivity across an entire network domain and remote sites. Utilized vulnerability scanning tools and systems to monitor vulnerabilities across platforms systems and devices to eliminate threats as they arise. Stood up WSUS and maintained the system for patch management throughout the entire landscape. Managed and maintained VMWARE vSphere and environment to maximize performance security and operability. Implemented encryption network wide for devices endpoints and servers to provide and comply with HIPAA policies and procedures. Segregated networks and wireless networks to provide authentication accountability and assurance across the entire landscape. Helped design and implement the network storage solution to assist with backup's reliability and redundancy. Maintained monitored and acted on network event threats and documented and implemented strong security protocols procedures and deployed automated attack vector responses to various threats Maintained and managed the spam appliance for email visibility and control into threats and attacks via email. Also configured the system for security and manageability. Maintained the firewall to advanced security policies and configurations to better defend detect and respond to threats. Crafting and keeping strong security policies and profiles to keep internal systems safe. Deployed and managed company VPN and profiles and policies to properly allow external access to internal resources securely. Investigated monitored and deployed network and system monitoring across platforms to have better insight into threats and vulnerabilities therein. SIEM, SYSMON Log management etc Worked with third party risk assessment companies (ECFIRST) to assess and develop maintain network security and policies to protect internal assets. Deep understanding of compliance and how to protect and guard various

systems to comply with various regulations. Maintained Microsoft exchange 2013 for the entire organization along with the entire active directory structure designing for security and monitored maintained all throughout. Proficient with latest Exchange 2016 and Active directory 2016 setup deployment and organization. Implemented KnowBE4 security awareness training and automated phishing alerts / training for staff including automated phishing schemes to teach and train users on attacks. Managed and maintained sizable Citrix environment for remote access and application deployment and security. Continuously utilizing latest technologies and attack techniques to assess various systems throughout the network to try and attack. And then building systems and rules and alerts to block, alert and manage the threats or deficiencies within the network Regulated and implemented Network Access Control to provide proper authentication to network and provide visibility within linking device to user and MAC address to monitor and manage devices and potential threats. Maintained the MDM (Mobile Device Management) software / solution to properly provision devices and to monitor and maintain security within the network and for external users and traveling employees. (SOPHOS MDM) Developed numerous PowerShell scripts to automate mundane and difficult tasks within the organization. Active directory user setup, Exchange email setup, Lync / Skype for business setups, Network drives and permissions, decommissioning servers, users etc Maintained workstation and server network security solution agents and systems software (Kaspersky, Symantec) and the policies and procedures within for highest security keeping usability and availability in mind allowing for seamless integration and usage especially for the end users. Spearheaded the remote access solution for any and all systems (VNC) for connecting to remote devices and servers anywhere you have an internet connection utilizing 2FA to authenticate. Experience IT Analyst DDG - Baltimore, MD May 2012 to August 2015 Maintain an office of approximately 100 machines and servers for daily operation and maintenance. Provide optimal software and application installation to keep workstations up-to-date and performing at peak speed and power. Help in the process of completely moving an IT Infrastructure from one office to another and setting up the new network from scratch in the new office. Perform on-site analysis, diagnosis, and resolution of complex desktop and printing problems for end-users, recommend and

implement corrective solutions. Install, configure, test, maintain, monitor, and troubleshoot end-user workstations and servers. Assess the need for and implement performance upgrades, including the installation of CPUs, I/O and NIC cards, hard drives, RAM, memory chips, CD-ROM's, etc. Collaborate with Director of IT to ensure efficient operation of the company's desktop computing environment. Perform hands-on fixes at the desktop level, including installing and upgrading software, installing hardware, and configuring systems and applications. Perform moves and initial user setups including profile and phone setups. Maintain an inventory of all monitors and workstations. Liaise with third-party support and PC equipment vendors. Assist in developing long-term strategies and capacity planning for meeting future desktop hardware needs. Education Bel Air High School - Bel Air, MD September 2015 to Present Kaplan School February 2012 Certificate TESST College of Technology - Baltimore, MD Skills ACTIVE DIRECTORY, DHCP, VMWARE, VPN, DNS, ENCRYPTION, EXCHANGE, FIREWALLS, HIPAA, NESSUS, SIEM, SNORT, WIRESHARK, DEPLOYMENT, SCRIPTING, VISUAL BASIC, LINUX, UNIX, SECURITY, NTFS Additional Information Key Skills * Currently studying for the latest security+ certification. * PowerShell programming and scripting & Remote administration (7 Years' experience) * Patching and Remote software management (WSUS, Batchpatch, PDQ Deploy etc ) * Perform red-team operations to further detect and mitigate breaches from a blue teamers perspective * Monitoring and utilizing tools like SIEM and network performance monitors for compliance and security. * HIPAA Privacy & Security * Deploying Wi-Fi solutions setup and configuration using best security practices and NAC. * Configuring firewalls and VPN connections for security and site to site connectivity * Maintaining and managing Spam appliances for email security * Deploying and configuring phishing and IT security training for staff * Active Directory & Exchange deployment and management for security; Group Policy DNS and DHCP * VMWare management and configuration * Encryption for network devices protocols, traffic and systems * Linux, Kali Linux and other for penetration testing and red-teaming. * NTFS Permissions * Wireshark, Nessus, Snort * Constantly and consistently learning as much as possible and joining webinars going to conferences and Following tech, latest breaches and techniques to stay current and on top of the IT Landscape

especially from a security analyst perspective. 4 Years System Administrator / Security Analyst for Ashley Inc. 3.5 years' experience as an IT Support / Helpdesk Analyst at an architectural firm. 12 years' experience operating Open Source Systems, Linux and UNIX; applications and Software. 2 years of Visual Basic Programming in High School. Excellent hardware/software technician. Skilled in Risk Assessments and remediation's.

Name: Hunter Snyder

Email: monicaallen@example.org

Phone: 001-648-689-9903x8795