Sr. Security Analyst Sr. Security Analyst Sr. Security Analyst - Howard University Hyattsville, MD Skilled Information Security Analyst with strong critical thinking skills. Fast learner and able to thrive in a fast-paced, team-oriented environment. Work Experience Sr. Security Analyst Howard University - Washington, DC January 2018 to Present Utilized Network auditing, and SIEM tools to perform investigations during security incidents. Assisted in performing internal audits in order to assure University was in compliance with HIPPA, PCI-DSS standards Worked directly with CISO to implement campus-wide VPN and multi-factor authentication solutions. Performed weekly litigation/eDiscovery requests on behalf of Office of the General Counsel (OGC) and other third party law firms affiliated with the University. Performed routine vulnerability assesment scans on production servers and gave mitigation recommendations to necessary parties. Analyst SOC - Fairfax, VA May 2017 to January 2018 Monitor and investigate alerts generated by SIEM tools. Reviewed logs to hunt for malware, traffic anomalies, and any compromise to the overall security posture of the network. Generate daily reports for senior management which include current real-world threats, a list of vulnerable network hosts, and recommendations on threat mitigation Perform semi-monthly scans on client network to asses critical vulnerabilities, and track network assets. Create and tune IDS/IPS rules to detect threats and reduce false positive alerts. Assist in creating Standard Operating Procedure documentation for use case scenarios. Lead daily teleconference meetings between SOC and client security team, in which notable incidents, ongoing investigations, and other collaboration topics are discussed. IT Specialist Cyberdata Technologies/U.S. Census Bureau - Herndon, VA August 2015 to June 2017 United States Provisioned users accounts in Active Directory Assisted networking team in troubleshooting VPN issues related to laptops assigned to US Census field representatives Assisted in configuring and managing digital certificates/virtual smart cards assigned to US Census field representatives. Provided phone and remote desktop support to end-users. Generated end-of-month reports that detailed the various incident types that were troubleshooted Analyzed event logs of proprietary applications in order to resolve issue or escalate issue to necessary personal Help Desk Analyst American Institutes for Research - Washington, DC June 2015 to August 2015 United States

Created detailed and accurate tickets using information provided by clients Initiated video conferencing sessions (Citrix GoToMeeting) sessions for executive meetings. Provided live support and troubleshooting. Coordinated equipment deliveries to various on-site buildings and off-site facilities Performed help desk operations such as account creation, computer re-imaging, and systems administration Assisted in imaging laptops to the specific needs and roles of onboarding employees. Organized and completed a cleanup of a 4 month ticket backlog Education Master of Science Western Governors University - Salt Lake City, UT 2018 Bachelor of Arts in Communications University of Maryland - College Park, MD 2014 Skills SECURITY (1 year), SIEM (1 year), IDS (Less than 1 year), IPS (Less than 1 year), CISCO (Less than 1 year) Additional Information Skills Snort IDS/IPS Rule Tuning Windows, Linux and Mac OS Packet Analysis (Wireshark, tcpdump) SIEM and Incident Review (Splunk/Splunk ES, Web Proxy, Next-Gen Firewall configuration and log McAfee Squert, Netwrix) analysis (BlueCoat, Cisco ASA, Palo Alto) Microsoft eDiscovery Vulnerability Assessment/Asset Tracking tools Strong communication skills and customer service (Nessus Security Center and Nexpose) experience Nmap, Burp Suite, Metasploit

Name: Amanda Brown

Email: hday@example.net

Phone: 001-878-550-7171x052