Job Seeker Arlington, VA Work Experience Intelligence Community Client October 2013 to Present Perform intrusion detection analysis on near real time network traffic to assess, characterize, and report malicious events in order to maintain network integrity Work incident response events and handle reported information spills Identify compromised systems and provide victim notification Coordinate with appropriate groups to clean infected systems and neutralize cyber threats Operations Manager National Security Agency - Fort George G Meade, MD January 2013 to October 2013 Defensive Cyber Operations: January 2013 - October 2013 Manage daily operations of large branch of computer network defense (CND) analysts defending Department of Defense (DoD) networks Lead analysis in high-profile network intrusion investigations Provide onsite incident response support to direct USG/DoD/DIB equities, leveraging knowledge of adversary techniques to triage ongoing cyber activity; providing stability to ongoing intrusions while recommending remediation actions Shape CND analytical and technical training pipelines Lead Cyber Threat Analyst December 2011 to January 2013 Analyzed near real-time network traffic for malicious activity on global-scale, multi-billion dollar DoD computer network in support of a 24/7 operation center environment. Collaborate with external U.S. Government Agencies and Industry partners in the Intelligence and CND communities Lead analytical collaboration across a global enterprise Reduced risk to DoD network through creative use of network-based malware and spear-phishing mitigation recommendations Cyber Threat Analyst March 2011 to December 2011 Analyzed exploits for mitigation recommendations Categorized and reported numerous malicious events containing actionable information for the CND and IC communities Increased intrusion detection capabilities through creation of network detection IDS rules IT Security Summer Intern Aspect Security, Inc - Columbia, MD May 2007 to September 2007 Investigated client internet security vulnerabilities Support penetration attempts on client websites Supported lab operations and maintenance of server hardware Education B.S. in Information Systems Radford University - Radford, VA 2010 Additional Information Key Competencies Network Intrusion Analysis Intrusion Detection Systems (IDS) Snort PCAP Analysis - Wireshark Cyber Intelligence Analysis & Reporting Netflow, Metadata Analysis Computer Network Exploitation Techniques Intrusion Prevention Java,

Java Script, SQL, Objective-C, HTML FireEye, ArcSight All Source/Open Source Analysis

Name: Elizabeth Herman

Email: bradshawchristina@example.org

Phone: +1-828-385-7080