Information Security Engineer Information Security Engineer Information Security Engineer - U.S. Department of Justice, FBI Terrorist Screening Center (TSC) Fairfax, VA Authorized to work in the US for any employer Work Experience Information Security Engineer U.S. Department of Justice, FBI Terrorist Screening Center (TSC) - Vienna, VA March 2015 to Present Integral team member assisting hardware refresh from Cisco IDS to Sourcefire IDS/IPS and migrating from a passive to inline deployment Responsible for patching, upgrading and configuring all IDS/IPS sensors to maintain information security posture at the TSC Regularly review government and open-source intelligence to extract malicious domain/IP indicators to create custom Snort rules in Sourcefire as well as create custom searches and reports in Splunk to alert on any malicious activity Configuration and maintenance of Splunk SIEM as well as Raytheon Trusted Gateway System (secure multi-directional data transfer solution) Perform daily monitoring, real-time data analysis, and event log correlation of security events utilizing Sourcefire and Splunk Develop and implement security policies and solutions architecture to mitigate risks and enhance system security Collaborate with security engineering and align with other team resources to proactively assess potential items of risk and new project vulnerabilities to mitigate and eliminate risk to TSC information assets Assist in the determination of security vulnerabilities, gather remediation requirements and recommend appropriate solutions Advise government managers on monthly events of interest; triage potential incidents, determine the nature and scope of the event/incident, as well as classify the severity and priority of the incident Present monthly security analysis/situational awareness reports and provide recommendations to management related to cyber security risk management and incident response Wireless Intrusion Detection System (WIDS) Analyst U.S. Department of Transportation, Federal Aviation Administration - Leesburg, VA May 2014 to March 2015 May 2014 - Mar 2015 Performed real-time data analysis of wireless intrusion detection system (WIDS) alerts and events generated by Mortorola Airdefense and Arcsight Regularly reviewed and monitored SIEM interface, as the data correlated and aggregated alert data from 1800+ remote sensors Identified, analyzed, and remedied WIDS alerts and reported findings to government Watch Officers (WO) Performed daily monitoring to ensure all remote sensors were

active and reported to field site personnel in the event of failure Promptly escalated and updated WO of anomalous rogue activity to mitigate further usage of unauthorized devices Security Operations Center (SOC) Analyst U.S. Department of Homeland Security, Immigration and Customs Enforcement - Chantilly, VA January 2013 to May 2014 Chantilly, VA Security Operations Center (SOC) Analyst Jan 2013 - May 2014 Performed front line triage, routing and tracking of security related incidents, events, inquiries, and a variety of other security related issues for the ICE SOC Responsible for containment, remediation and prevention of any data spillage occurances over the ICE network Reviewed security alerts and events generated by a variety of network and host based security appliances (Firewalls, NIDS, HIDS, Bluecoat proxy logs via Splunk, System logs) and determined correct remediation actions, filtering, and escalation paths Performed real-time data and traffic analysis using IDS/IPS systems such as ISS Proventia and packet capture data analysis using Wireshark Coordinated and liaised with other DHS components with information regarding intrusion events and security incidents Assisted with the development of Tactics, Techniques and Procedures (TTP) documentation to assist with personnel training of SOC tools and daily operations Regularly reviewed open-source security publications and blogs for Zero-days and other cyber related threat indicators to remain vigilant of emerging threats that have a potential to disrupt organization security posture IT Specialist U.S. Department of the Treasury & Consumer Financial Protection Bureau - Washington, DC October 2011 to January 2013 Oct 2011 - Jan 2013 Provided desktop support to 5,000+ end-users for the U.S. Department of Treasury and Consumer Financial Protection Bureau by researching, analyzing, and resolving hardware, software, and network issues received by phone and email via Remedy Performed installation of desktops, laptops, peripherals, and software products for networked, classified and unclassified, and standalone environments Performed system refreshes for over 300 Consumer Financial Protection Bureau hosts Provided software support for multiple Treasury-approved applications used for financial and litigation purposes Utilized InTrust to track compliance within the environment and to review Windows OS system level event logs for servers and desktops for unauthorized activity Evaluated and tested applications and software development procedures to ensure program

functionality according to user requirements and established guidelines Managed patch deployment through configuration management and software distribution tools (SCCM) Regularly reviewed current patch levels of desktops/servers to identify systems failing to receive patches and remediated as necessary Managed AD accounts and placed workstations in appropriate OU containers Education B.S. in Applied Information Technology George Mason University - Fairfax, VA 2017 A.S. in General Studies Northern Virginia Community College - Annandale, VA 2008 Additional Information TECHNICAL PROFICIENCIES Operating Systems: Windows 7/8/Server 2012 R2, Linux, Mac OS X Networking: TCP/IP, LAN/WAN, VPN, Routers, Firewalls Platforms/Servers: Cisco FireSIGHT (Sourcefire), Snort, Splunk, Raytheon Trusted Gateway System, Motorola Airdefense, Intrusion Detection and Prevention Systems (IDS/IPS), Host and Network Intrusion Detection Systems (HIDS and NIDS), Active Directory (AD), System Center Configuration Manager (SCCM), Dynamic Host Configuration Protocol (DHCP), Domain Name System (DNS) Software: Cisco IPS Manager Express, IBM Internet Security Systems (ISS) Proventia, McAfee ePolicy Orchestrator, IBM BigFix, Wireshark, HBGary, RegRipper, VMware eSXI, Nmap, BMC Remedy, Putty, SCP, GuardianEdge

Name: Christopher Murphy

Email: gbuchanan@example.com

Phone: 5247096279