Information Security Analyst Information Security Analyst Information Security Professional Helena, MT Authorized to work in the US for any employer Work Experience Information Security Analyst State of Montana Department of Justice - Helena, MT February 2016 to Present Worked with the Information Security Officer to develop an information security program for the Montana Department of Justice. Drafted and implemented policies and procedures. Implemented network security monitoring solutions (Snort, Bro, Enterprise Log Search and Archive, and OSSEC). Participated on multi-agency work groups in evaluating policies and endpoint security solutions for all State agencies. Responded to and analyzed security events and escalated to incident status as necessary. Support Department of Justice divisions with federal audits and assisted with maintaining compliance with federal requirements. Maintained compliance with the FBI Criminal Justice Information Systems (CJIS) Security Policy and Montana state policy based on NIST SP 800-53. IT Security Analyst Noble Drilling Services Inc - Sugar Land, TX July 2015 to January 2016 Responsibilities Performed both day-to-day operational security tasks and managed projects to bring Noble s IT security program in line with the NIST Cybersecurity Framework. Wrote and implemented policies and procedures. Conducted risk assessments with other business units. Supported Noble security awareness training by conducting phishing training exercises and writing training material. Worked with Blue Coat web filtering, OpenDNS, Bit9 application whitelisting, Malwarebytes, and FireEye. Evaluated new technologies for future implementation (next generation firewalls, SIEM, and vulnerability management solutions). Accomplishments Wrote policies and procedures for vulnerability assessment and encryption. Conducted a proof-of-concept with three vulnerability scanning vendors. Conducted risk assessments for IT programs in different departments. Skills Used Intrusion analysis, project management, packet analysis, endpoint security, application whitelisting, web filtering, risk assessments, technical writing, policy and procedure documentation. Cyber Security Analyst Apache Corporation - Houston, TX February 2014 to July 2015 Responsibilities Part of a three-person team responsible for the development and implementation of Apache Corporation s CyberSecurity group. Communicated with end users to develop plans on how to best secure their systems and tools without negatively impacting their work.

Analyzed intrusion alerts in Sourcefire, RSA Security Analytics, QRadar, and Splunk. Deployed multiple new tools as we expanded our security program, including endpoint security (Cylance) and data loss prevention (Digital Guardian). Performed tuning, routine maintenance, and updates on our security tools. Handled any support tickets concerning information security matters, including reports of phishing e-mails and infected systems/incident response tickets. Conducted incident response for malware infections in the environment. Compiled weekly reports on intrusion activity for senior management. Pending Secret clearance through the Private Sector Clearance Program. Accomplishments We updated our IPS infrastructure, we deployed a next-generation endpoint protection solution, and we deployed a data loss prevention platform. I am confident that, because of our work, the Apache Corporation's security posture is in a much improved state than it was in when we joined. Skills Used Intrusion analysis, systems administration, packet analysis, incident response, data loss prevention, endpoint protection, malware analysis Network Security Analyst Alert Logic - Houston, TX July 2013 to February 2014 Monitored intrusion detection systems for a variety of customers. Analyzed security events and logs to identify threats to customer networks while meeting service-level agreements. Managed customer cases with Salesforce to troubleshoot customer problems and identify ways to remediate potential threats. Conducted real-time analysis of SQL attacks, brute force attacks, malware, Trojans, and other threats to network security. Maintained Snort IDS sensors across numerous customer sites. Performed analyses with tools like tcpdump, NMAP, Wireshark, tshark, Snort, and Barnyard to effectively analyze, troubleshoot, and support Alert Logic intrusion detection systems. Systems Engineer Praemittias Defense Solutions - Hanover, MD August 2011 to July 2013 Assisted senior software developers with a variety of projects, including development and testing of GPS and wireless survey tools for mobile devices. Researched emerging technologies for use in current and future software development. Implemented and maintained a virtualization system for vulnerability research, product demonstrations, and CNO/CNE software development and testing. Built virtual environments and a Jenkins continuous integration platform for working with a subversion repository to compile code, run unit tests, and report on successes and failures. Supported training for SIGINT courses

covering wireless network analysis and collection. Programmed automation scripts and small programs in Python. Performed vulnerability assessments and penetration tests on local and global networks for a variety of clients. Compiled reports and documentation covering the results of the penetration tests and recommended remediation plans for any vulnerabilities discovered on the network. Active Top Secret clearance. Education Master of Arts in Forensic Psychology Marymount University - Arlington, VA May 2011 Bachelor of Arts in Psychology University of Colorado at Colorado Springs - Colorado Springs, CO May 2009 Associate of Arts Pikes Peak Community College - Colorado Springs, CO August 2007 Skills IDS/IPS (5 years), Vulnerability assessments (6 years), Linux/UNIX (7 years), Windows (7 years), Packet analysis (5 years), Risk Management (3 years), Risk Assessment (3 years), Policy Development (4 years), Process Development (4 years), Awareness Training (4 years), NIST (2 years), CJIS (2 years), Cyber Security, Information Security, CISSP (Less than 1 year), GCIH, GCIA, CASP Awards Nominee - Governor's Award 2017-12 Nominated by the Montana Department of Justice for the annual Governor's Award for my work deploying a network security monitoring program and developing network security monitoring processes and procedures. Certifications/Licenses Network+ June 2012 to August 2022 Security+ August 2012 to August 2022 CASP August 2016 to August 2022 CompTIA Advanced Security Professional GCIH March 2017 to March 2021 GIAC Certified Incident Handler CISSP January 2018 to January 2021 GCIA July 2018 to July 2022 GIAC Certified Intrusion Analyst Groups MS-ISAC March 2016 to Present Infragard August 2014 to Present

Name: John Thomas

Email: awilson@example.com

Phone: 001-778-684-9497