Al Larkin

23391 Roman Track, Boston, MA ♦ Phone: +1 (555) 513 7713

EXPERIENCE

APPLICATION SECURITY TESTER

New York, NY
02/2016 – present

- Provide mentoring for junior level analysts and specialists
- Aid team members for enhancement and enrichment of security monitoring tools with contextual information
- Lead cyber investigations for escalated, complex computer security incidents using computer forensics, network forensics, root cause analysis and malware analysis
- Develop tactical and strategic cyber intelligence by acquiring threat intelligence and technical indicators from external and internal sources
- Engage in threat hunting activities to proactively search for threats in the enterprise environment
- Create and maintain playbooks used in response for investigation/incident triggers in support of 24/7 Cyber Threat Operations and Cyber Threat Management program
- Create and maintain use cases for recurring investigation/incident triggers in support of the 24/7 Cyber Threat Operations and Cyber Threat Management program

SECURITY ASSESSMENT TESTER

Detroit, MI
04/2010 – 11/2015

- Location will be Bethesda or McLean
- Develop and document security evaluation test plan and procedures
- Assist in researching, evaluating, and developing relevant Information Security policies and guidance
- Actively participate in or lead technical exchange meetings and application review boards, documenting actions items/results of these events
- Conduct hands-on security testing, analyze test results, document risk, and recommend countermeasures
- Develop, assemble, and submit C&A testing results reports that document testing activity and results to support the creation of C&A risk assessments and C&A approval packages
- Assess/calculate risk based on threats, vulnerabilities, and shortfalls uncovered in testing

CLOUD SECURITY TESTER

Philadelphia, PA
12/2004 – 12/2009

- Search for the security testing standards and make use of them
- Help the organization build information security awareness e.g. by providing trainings
- Align security test activities within project lifecycle activities
- Knowledge of threat modeling and other risk identification techniques, Knowledge of system security vulnerabilities and remediation techniques
- Analyze a given situation to determine which security testing approaches are most likely to succeed, implement them and evaluate the effectiveness
- No restriction for travelling
- Demonstrate the attacker mentality by discovering key information about a target, performing actions in a protected environment that a malicious person would perform and understand how evidence of the attack could be deleted

EDUCATION

GEORGETOWN UNIVERSITY

Bachelor's Degree in Computer Science

SKILLS

- Demonstrated proficiency in basic computer applications, such as Microsoft Office software products
- Knowledge of the incident handling procedures and intrusion analysis models
- Ability to travel, occasionally overnight
- Industry certifications in general technology (e.g. Microsoft Certified Professional (MCP), Microsoft Certified Solutions Expert (MCSE), Network+)
- Ability to work independently with limited supervision
- Ability to formulate, lead and persuade individuals, large teams and communities on ideas, concepts, and opportunities
- Advanced knowledge of processes, procedures and methods to research, analyze, and disseminate threat intelligence information
- 5+ years in information security with specific application security testing experience
- Demonstrated experience with systems for automated threat intelligence sharing using industry standard protocols such as Structured Threat Information Expression (STIX) and Trusted Automated Exchange of Indication Information (TAXII)
- Consistent history of delivering on commitments