LOGIN.GOV

Performance Profile: Login.gov Security Engineer (Security Analyst Technical Expert)

Opportunity Overview

This opportunity is located in the Technology Transformation Services (TTS) Solutions Division's Login.gov team. The Login.gov team is remote-first and is composed of experts across product development, software engineering, cybersecurity, and platform engineering.

Login.gov is a FedRAMP authorized secure sign-in service created for the public to access participating government agency sites, products, and services. At its core, Login.gov is both an authentication and identity verification service and is now available to all levels of government: federal, state, and local.

Position Summary (Public)

As a security analyst technical expert, you will report to Login.gov's security branch chief. In this fully remote position, you will work closely with Login.gov's product and platform teams to improve Login.gov's defensive capabilities. You will play a key role in helping Login.gov's security team implement best practices to protect user data, secure Login.gov's application and infrastructure, and combat fraud and abuse. You will provide strategic guidance to Login.gov's leadership team, provide feedback on security program objectives, and lead improvements to Login.gov's cybersecurity practice.

Key Objectives

Objective #1: Provide subject matter expertise on cybersecurity practices to Login.gov Leadership

- Demonstrate expertise in security industry standards (e.g., NIST 800 series) and best practices
- Demonstrate expertise in developing standard operating procedures for securing Software as a Service applications
- Knowledge of software product delivery in a federal DevOps environment.
- Experience with cloud architecture and data workflows
- Communicates with internal and external partners to share Login.gov's security posture, risk, and operational processes.
- Contribute to security program goal setting and roadmapping activities.

Objective #2: Contribute to Login.gov's Cybersecurity Practice

- Demonstrate expertise with security activities such as vulnerability testing and analysis, incident response and analysis, alert response and analysis
- Demonstrate expertise in conducting data analytics activities to support monitoring, detecting, defending against, or responding to security incidents.
- Demonstrate expertise in scripting using object-oriented languages (e.g., Python) to automate data analytics or business processes
- Collaborate with application development teams, platform engineers, and Security Operations Center (SOC) engineers to build and implement security in an open source, live services environment
- Collaborate with User Experience, Infrastructure, and Application Developer Engineers to ensure changes to Login.gov's product or infrastructure do not negatively impact security

Objective #3: Ensure Login.gov maintains its FedRAMP authorization

- Demonstrate expertise in maintaining systems that comply with NIST-800-53 controls.
- Demonstrate expertise in developing and maintaining artifacts for cybersecurity assessments
- Demonstrate expertise in participating in technical interviews for cybersecurity assessments.
- Demonstrate expertise in preparing application developers, site reliability engineers, or platform engineers for technical assessment interviews
- Propose changes to Login.gov development and site reliability engineering practices to better support automated compliance

Objective #4: Collaborate effectively on distributed, agile teams

- Openly share knowledge and work collaboratively to integrate anti-identity fraud principles into product and engineering practices.
- Participate in regular retrospectives and provide feedback to help improve the way the team works.
- Maintain a work environment of respect, diversity, equity, inclusion, accessibility, mutual support, flexibility, collaboration, continuous learning, and commitment to customer / partner needs. Ensure all perspectives are valued and included. Uphold TTS values of inclusion, integrity, and impact.