Performance Profile: TTS DevTools Security Engineer

Opportunity Overview

This opportunity is located in the Technology Transformation Services (TTS) Solutions Division's Accelerators portfolio on the new DevTools team. The DevTools team is remote-first and forming a small cross functional team with skills including platform engineering, application development, security engineering, and product management.

The DevTools mission is to provide shared tools and services that allow TTS teams (such as USA.gov, Login.gov, Cloud.gov, and 10x) to ship digital services quickly, easily, and sustainably. DevTools works to make the right thing the easy thing, greatly reducing the effort needed to develop and operate delightful, secure, and compliant digital services to the American public.

Position Summary (Public)

As a Security Engineer in DevTools, you'll be part of a cross-functional team to deliver developer-centered products using agile methodologies and modern software development practices while building capacity for product innovation in government.

The Security Engineer focuses on putting the *SEC* in DevSecOps by baking security guardrails into DevTools services and in turn, everything they are used to develop.

Security Engineers on our team are:

- Experienced with securing cloud based services with high security and compliance requirements.
- Experienced with security tools and practices used in development and continuous deployment, including SAST, DAST, and scanning of dependencies and artifacts.
- Experienced with securing continuous integration, delivery, and deployment systems.
- Experienced with at least one development language (Javascript, Python, Ruby, etc) or IaC tool (Terraform, Pulimi, etc).
- Experienced securing production solutions based on IaaS and PaaS offerings from AWS, Azure, and/or GCP.
- Eager to automate away compliance burden and use a risk based approach to making sound investments in security.

Key Objectives

Objective #1: Secure services, tools, patterns, and components for community use

- Apply security engineering principles in all aspects of design, development, and operation of DevTools services and offerings.
- Add security tooling and guardrails to CI/CD pipeline components.
- Facilitate use of threat modeling, threat hunting, and chaos engineering approaches to improve the security of DevTools services and level up capabilities of the DevTools teams.

- Work with the team to meet quality standards for any product you build.

GS-15

- Technical leadership in securing platforms and cloud infrastructure.
- Facilitates team decision making based on complex constraints and data.
- Sharing technical expertise with team members and users through pairing, examples, documentation, and presentations.
- Extensive skill in securing cloud based digital services based on open source, in-house developed code.
- Extensive experience with compliance processes, and partnering with compliance oversight and auditing teams, and advocating for risk based approaches to compliance.

Objective #2: Developer, platform, and compliance support

- Review DevTools products in use with real and sample services and look for areas of improvement to defense and safety.
- Use qualitative and quantitative data from systems and developers to improve the security of DevTools services and the services that depend on them.
- Work closely with platform engineers to bake security into the platform, meet and exceed compliance requirements, and reduce burden on developers.
- Work closely with application engineers to bake security into developed applications and add guardrails and helpers to make secure development easier.

GS-15

- Reduce cognitive load for all engineers in TTS through creation and refinement of reusable, tested, secure, and compliant security tools and guardrails.
- Regularly interact with the TTS security and compliance community and beyond to inform DevTools efforts and share our capabilities.

Objective #3: Work effectively in the federal government

- Develop and maintain knowledge of software factory and platform concepts and how they are leveraged in government.
- Understand risk management frameworks and Authorization to Operate (ATO) concepts.
- Keep up-to-date on policies, regulations, and requirements that impact digital services, and seek ways in which DevTools can reduce the burden of these requirements on digital service teams.

GS-15

- Apply expert knowledge of and expertise in driving and implementing technology solutions that overcome significant challenges resulting from complex or bureaucratic environments or technically difficult problems.
- Apply expert skill in developing and maintaining positive relationships at various levels within an organization and championing diversity, equity, inclusion, and accessibility.