ENSURING SECURITY IN A CLOUD-FIRST ENVIRONMENT

Problem:

- Lack of next-generation unclassified software development environment
- Consolidating numerous independently run government and contractor labs and hosting environments into a single environment that could better detect insider and external threats to their organization

Solution:

- The customer's technical staff finally had self-service access to create the resources they need for their projects
- Resource usage maintained within budget and aligned with compliance standards such as FedRAMP

Customer Challenges

The national security customer of our cloud infrastructure specialists at Applied Insight required a next-generation unclassified software development environment. It needed to enable tens of thousands of users access to the resources they needed to build new internal applications and contribute to open source projects. The customer wanted to consolidate numerous independently run government and contractor labs and hosting environments into a single environment that could better detect insider and external threats to their organization.

AI Solution Features

Applied Insight proposed an infrastructure-as-code solution with a heavy emphasis on automation to speed development and reusability and lower support costs. Security was paramount and at the center of the overall solution. Applied Insight designed, deployed, and maintained this next-generation unclassified development environment built solely on AWS. This secure and scalable environment provides centralized DevOps services such as SCM and CI across the entire organization.

Benefits to the Customer Mission

- The customer's technical staff finally had self-service access to create the resources they need for their projects

- Resource usage maintained within budget and aligned with compliance standards such as FedRAMP