Section: PUBP-6727

Mutual Monitoring in the Cloud Evaluation Plan

Alexander Stein
astein38@gatech.edu

Summary

The project, as detailed in the intial proposal, examines the many challenges to effective multi-party security monitoring of cloud service providers and designing a solution based on two areas of work. The first area of work is an analysis of best-in-class contemporary techniques for multi-party cloud security monitoring, typified by FedRAMP's administration of their Continuous Monitoring Program. The second area of work, informed by the first, is a specification and prototype for a novel architecture for multi-party security monitoring of cloud service providers, addressing challenges and shortcomings identified from the first work area.

To evaluate the solution, I plan to use a multi-disciplinary approach to assess the project's final deliverables, identifying benefits to the proposed solutions; confirm and discover limitations to the solution; and propose future areas of work. I categorize this multi-disciplinary approach into qualitative and quantitative methods, which I describe in more detail below.

Quantitative Methods

Evaluating this project will include the quantitative methods below.

1. Model the range of costs for continuous monitoring process, data access, and submission for FedRAMP's current requirements.
2. Model the range of duration for processes related to continuous monitoring activities for FedRAMP's current requirements.
3. Model and estimate the equivalent processes in the proposed mutual monitoring architecture.

Qualitative Methods

Evaluating this project will include the qualitative methods below.

1. Identify challenges and obstacles to current FedRAMP continuous monitoring processes through resources including. but not limited to:
    - literature review of multi-party security monitoring of cloud service providers, as FedRAMP and other regulatory frameworks implement it;
    - sentiment analysis FedRAMP's official forum for its 20x modernization program, in which stakeholders often critique current processes.
2. Use data from 1 to identify features and use cases of the mutual monitoring architecture to address identified challenges with a qualitative analysis of their positive or negative impact.
3. Interview stakeholders with different roles in FedRAMP authorizations and continuous monitoring. Participants will answer questions regarding the relevance and impact of challenges identified and benefits of the mutual monitoring solution's features to their work. The final report will summarize qualitative analysis of their answers to model how a mutual monitoring ecosystem will benefit the persona the stakeholder represents in the ecosystem.