Assessment workflow

This document defines Inference's approach to a security assessment, which we aim to follow in all our client engagements.

0. From contact to contract

To begin with you will be asked to fill-in our client on-boarding questionnaire and return it to us. We will then examine it and, if we think we can deliver upon it, we will tell you when, if not we will explain why not.

We shall agree with you the scope of the assessment (such as code repositories, subcomponents thereof, technical specifications) and its goals. This will normally take place during a call to determine what makes the most sense from a risk and return-on-investment perspective. The goals of the assessment may vary: from "find bugs in this code tree" to "find out how secure this protocol is", or "verify that this code correctly implements this protocol".

We shall then proceed with administrative formalities, namely the signature of a statement of work (SoW) and a service agreement. At this point we shall schedule a suitable date for a kick-off call.

1. Kick-off

We will organize a kick-off call with your technical team, to agree on:

- **The scope**. For example, the branch of the git repository and commit version, the third-party dependencies to review, if any.
- **The security goals and assumptions**. For example, if a smart contract is written in a high-level language and compiled to a lower-level language, is the compiler trusted or should we review the compiled code? If your project includes cryptography, is the code expected to be safe against side channels?
- **The reference documentation**. To save time, we recommend that your team prepares a list of links and documents that we can use to understand your system, how to use it, a "ground truth" describing how the system is expected to behave.
- **Communication aspects**. As we will have questions and observations to report, we prefer to communicate in a group chat. We shall provide a communications platform with end-to-end encryption, but we can also use your company's platform at your discretion. We may also organize weekly calls to discuss the progress and outstanding issues should the communications platform not suffice.
- **The reporting policy**. Would you like us to report findings as we go, so that your team can address them as early as possible, or only in the final report?

During the kick-off call, we also expect your team to walk us through your code base, or documentation, and answer our preliminary questions.

2. Assessment work and reporting

Inference staff performs the technical work, including tasks such as manual code review, dynamic analysis, use of automated tools, as well as review of the documentation and related literature, as applicable.

We will report our findings and hold regular calls, or other suitable information sharing method, as agreed with your team.

3. Preliminary report delivery

Inference delivers a report describing the security shortcomings which have been found, including a description, a severity rating (exploitability and impact), and mitigation recommendations.

The report is aimed at technical staff familiar with the code base, and includes an executive summary along with our general risk assessment.

4. Feedback and mitigation

Your team reviews our report and informs Inference of any concern over our analysis or severity rating. If needed, we will then organize a call to resolve outstanding issues. For example, we may discuss with your team how to best plan and prioritise mitigation measures, based on the perceived risks.

5. Fixes review and final report delivery

Inference reviews the mitigation measures implemented, and updates the report accordingly, adding a description of the status of each finding initially reported (for example, describing the mitigation implementation and the rationale behind it). The report will always indicate both the initial assumptions and the risk profile to better frame the findings.

Should you wish to publish the report, we will coordinate the announcement, agreeing on a publication date and contents to be published.