🧪 Solutions Engineer Take-home Assignment

This take-home test is designed to evaluate your ability to understand customer problems, assess relevant solutions, and effectively communicate technical information both in writing and through a demo.

First Challenge

Challenge: Review Blockaid's End User Protection Offerings and recommend two of the most relevant solutions to a wallet customer's needs. Provide a written explanation and API demo of the most relevant offerings.

Blockaid Product

Blockaid Information (request access):

- End User Overview: https://docs.blockaid.io/docs/enduser-overview
- API Reference Doc: https://docs.blockaid.io/reference/openapi-schema

Blockaid Offerings to Consider (based on API reference endpoints):

- Dapp Scanning
- Transaction Scanning
- Token Scanning

Customer Case Study

A cryptocurrency wallet is facing challenges with users losing funds to malicious actors. Specifically, they find many users reporting that their wallets are being drained by websites that advertise free airdrops. The most common attack that occurs is an unlimited ERC20 approval that is unknowingly signed by the user.

They are looking for solutions that can prompt users on the dangers of certain interactions that include some detailed information about why a specific asset interaction (asset being a generic term for anything a wallet can interact with) is dangerous.

Their previous DIY attempts at blocking malicious assets in the wallet was unsuccessful due to:

- A failure of their team to flag all dangerous assets comprehensively (false negatives) and a high number of false positives that frustrated customers
- A warning pop-up that didn't convey enough information. Many users would bypass the warning due to a belief it was a false positive, often at the instruction of a scammer.

- An inability to detect malicious assets before they begin stealing from users. Most malicious assets are only flagged after user losses are reported.

Take-home Instructions

1. Craft a short response (no more than 500 words) to the client to identify the TWO MOST RELEVANT Blockaid offerings to solve their problem. Give a short explanation for why these offerings will solve their problem and how it will overcome the issues they experienced with their DIY attempt.
    a. Hint: focus on reading the knowledge section

Second Challenge

Challenge: Review the smart contract of a stablecoin client and recommend security monitoring configurations based on the Blockaid monitoring platform capabilities. Provide a written recommendation for the configurations including invariants.

Blockaid Product

Blockaid Information (request access):

- Platform Visibility: https://docs.blockaid.io/docs/introduction-to-the-blockaid-platform (light on details but gives you an idea of what our platform does with monitoring)
- For the purposes of this worktest, assume our monitoring platform is capable of configuring any custom monitor in turing-complete code with inputs from both threat intel (able to identify known malicious addresses and exploit contracts) and on-chain state/events (seeing all confirmed transaction details along with the latest contract state).

Customer Case Study

Circle wants Blockaid to monitor the **USDC** stablecoin for potential security risks.
Token: 0xa0b86991c6218b36c1d19d4a2e9eb0ce3606eb48

They are especially concerned about:

- **Privileged access** (who can do what)
- **Proxy implementation upgrade risks** (details on upgradeable contracts here)
- **Potential for abuse of admin or role-based functions**

Take-home Instructions

In order to be onboarded, a solution engineer must analyze the smart contract and do the following:

1. Determine if there are any privileged roles in the contract (Owner, Pauser, etc.) and if so, what are they called?
2. Determine if there are any functions that are controlled by privileged functions (ex: onlyRole, only Owner modifier).

Submit a list of Privileged functions and the roles required to call them.

Use this information to suggest **access control detection rules** that can alert the client to suspicious activity. From this research, you should be able to help the client configure access control detection rules to ensure they are able to monitor for any breaches.

Feel free to ask questions for guidance on your takehome.