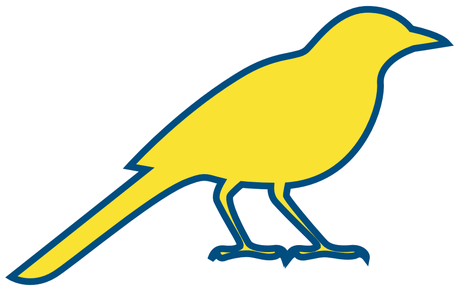
Detecting Nation State Cyberattacks with Classified Threat Sensors

Dr. Steve Weis, Dr. Aloni Cohen, Dr. Amina Asim

Private companies must defend against foreign nations without access to classified threat intelligence.

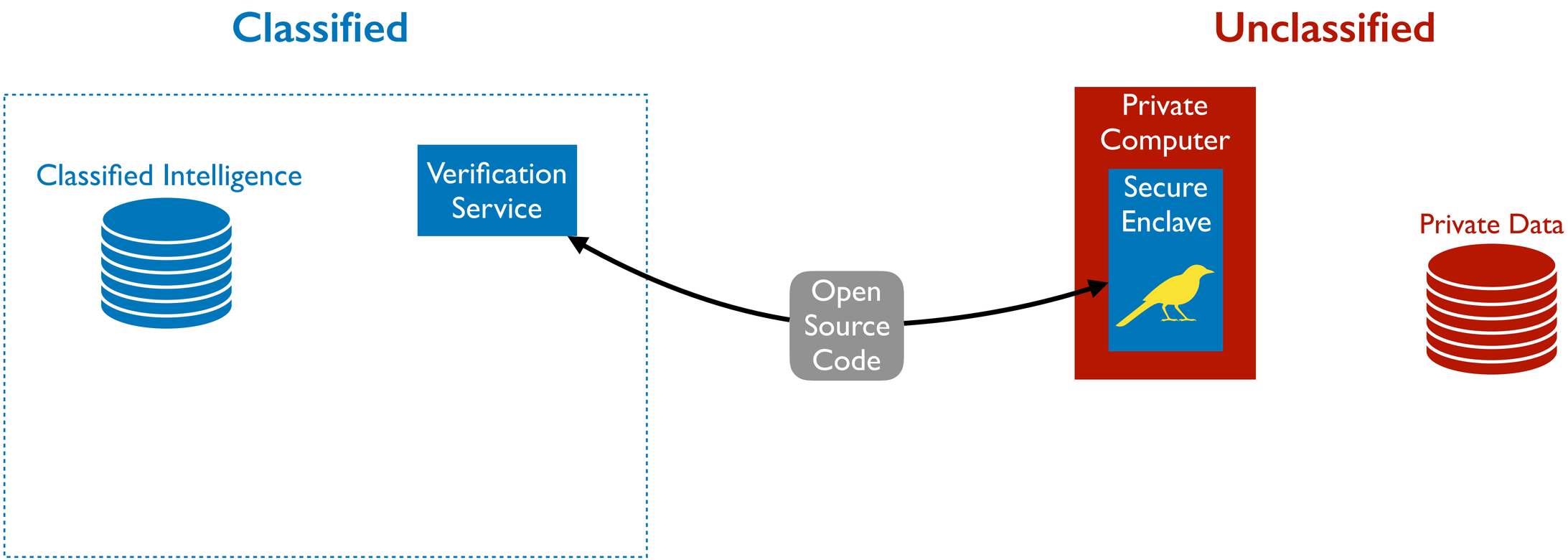
What if a *classified threat sensor* could apply classified intelligence to private company data?



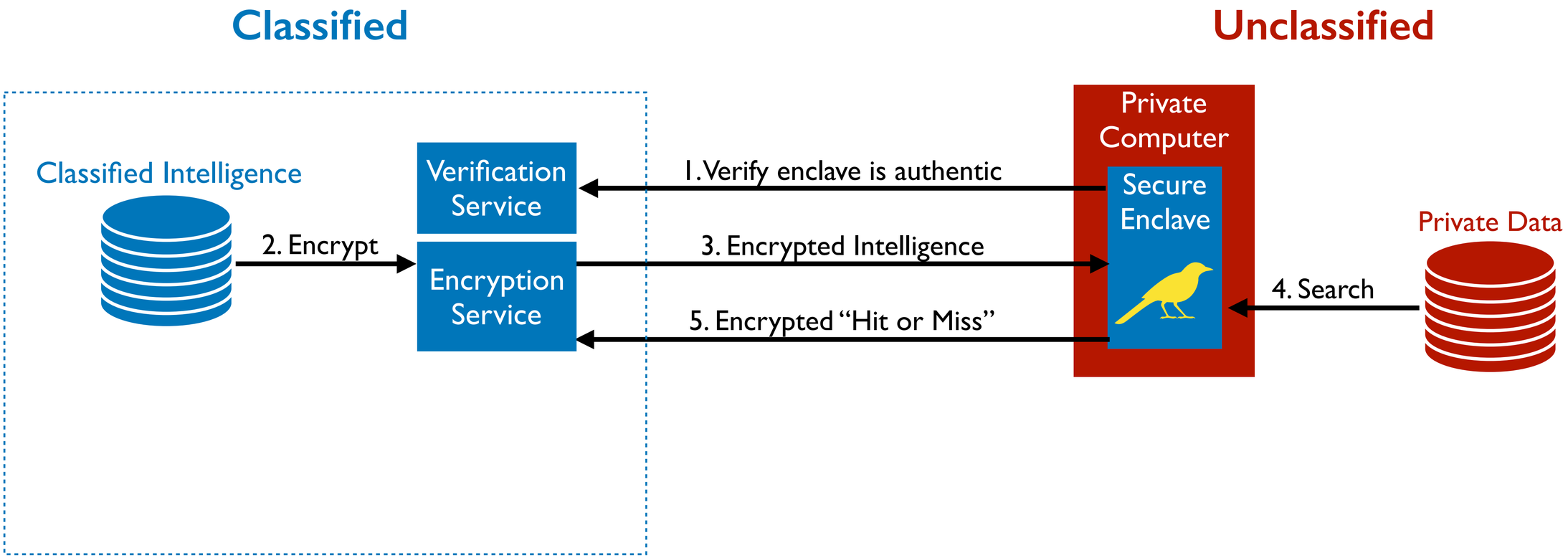
CANAREE: Classified Analysis of Network Attacks in a Restricted Execution Environment

Secure enclaves are safe spaces to run your own software on someone else's computer.

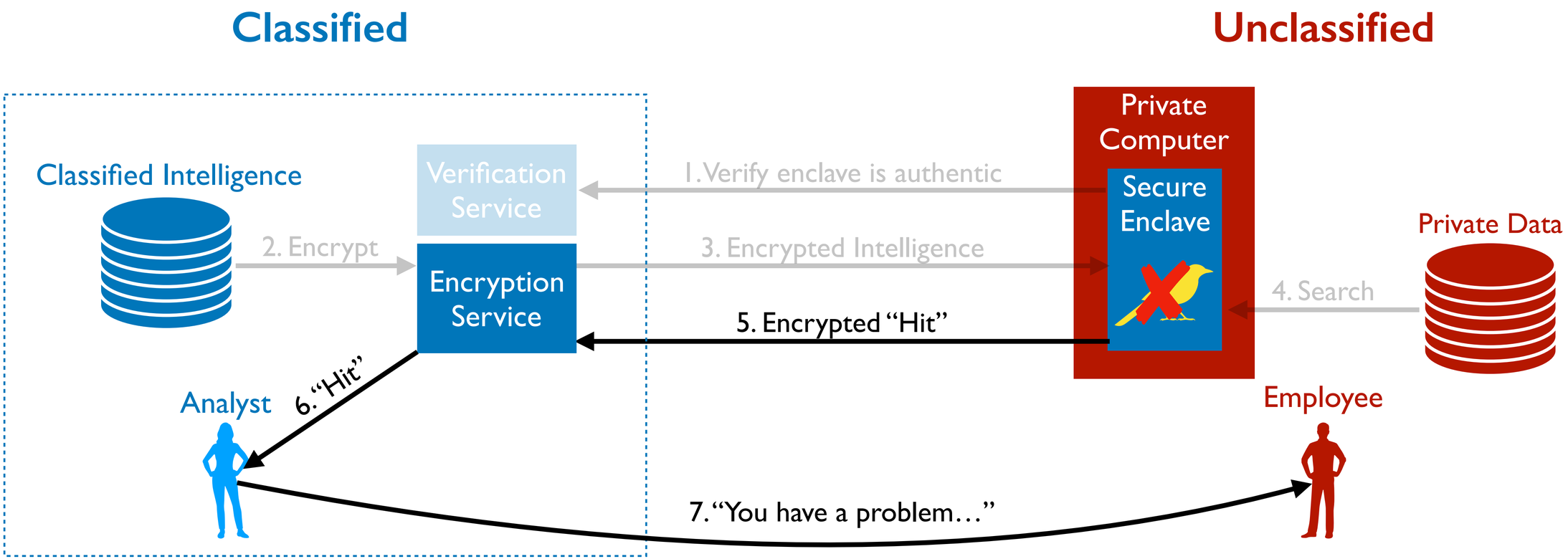
Starting a Classified Threat Sensor



Searching for Threats in Private Data



Responding to Detected Threats



The Good News:

You already paid for this technology.

Five Phase Plan

Phase 1	Open Source Proof of Concept
Phase 2	Industry-to-Industry Trial Deployment
Phase 3	Government-to-Government Trial Deployment
Phase 4	Government-to-Industry Unclassified Sharing
Phase 5	Government-to-Industry Classified Sharing

Calls to Action

Phase 1: Open Source Project

- Fund development.
- Contribute or review code.
- Offer compute testbeds and sample data.

Phase 2: Industry Trial

- Commit to a trial program with an industry peer.
- Publish results of trial.
- Share bug fixes.

Phase 3: Government Trial

- Commit to a trial deployment with a peer agency.
- Publish results of trial.
- Share bug fixes.