Detecting Nation State Cyberattacks with Classified Threat Sensors

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

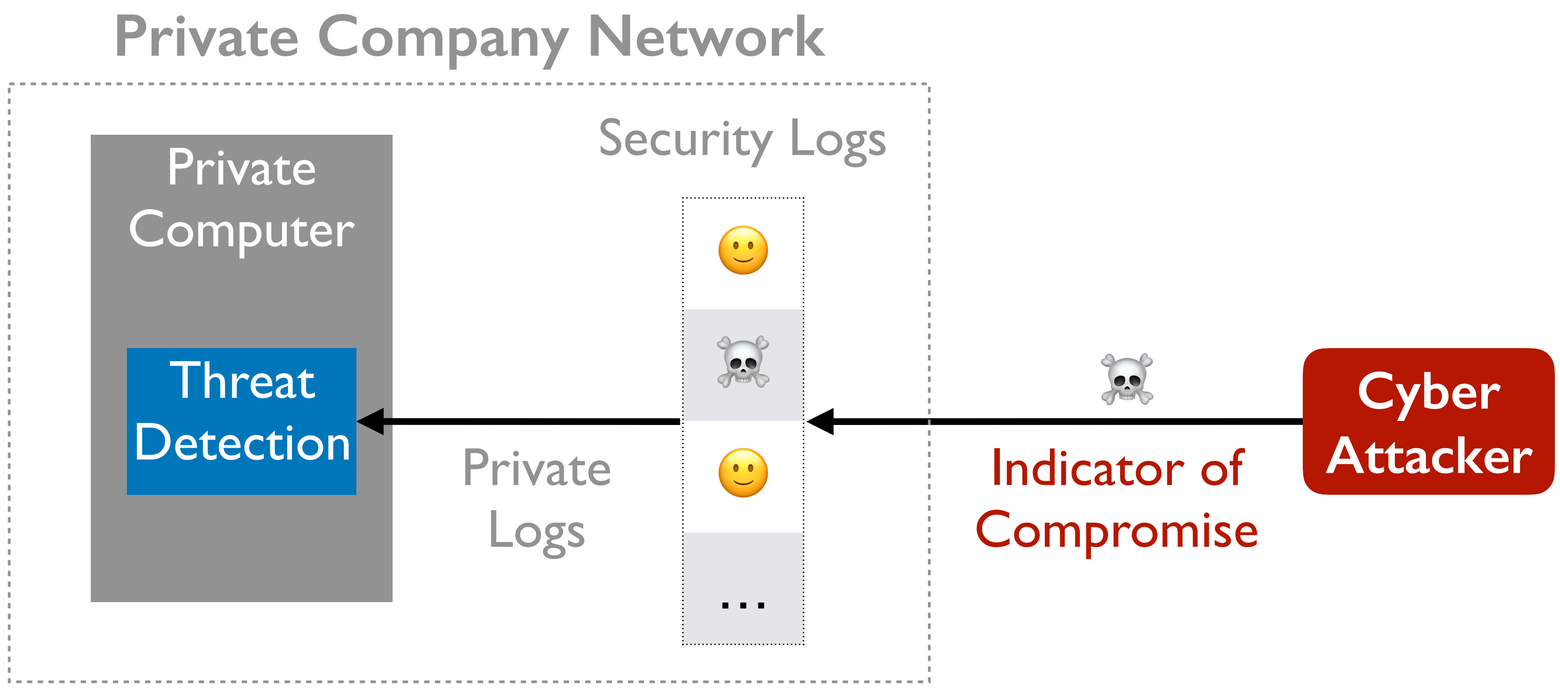
Dr. Stephen Weis

Dr. Aloni Cohen

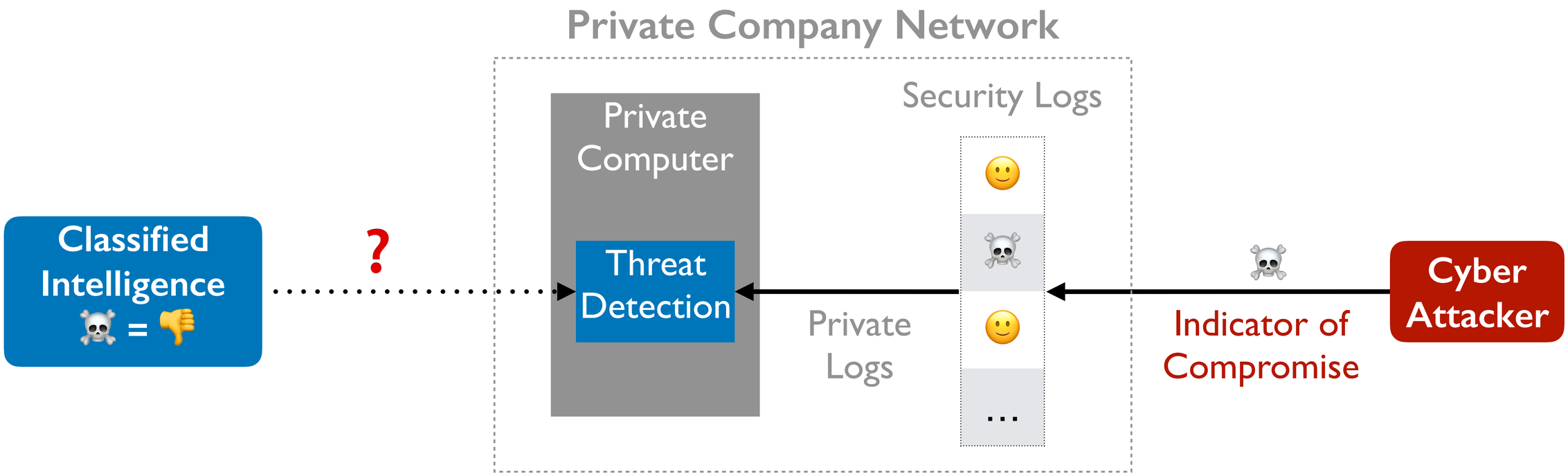
Dr. Amina Asim

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

The Information Sharing Challenge



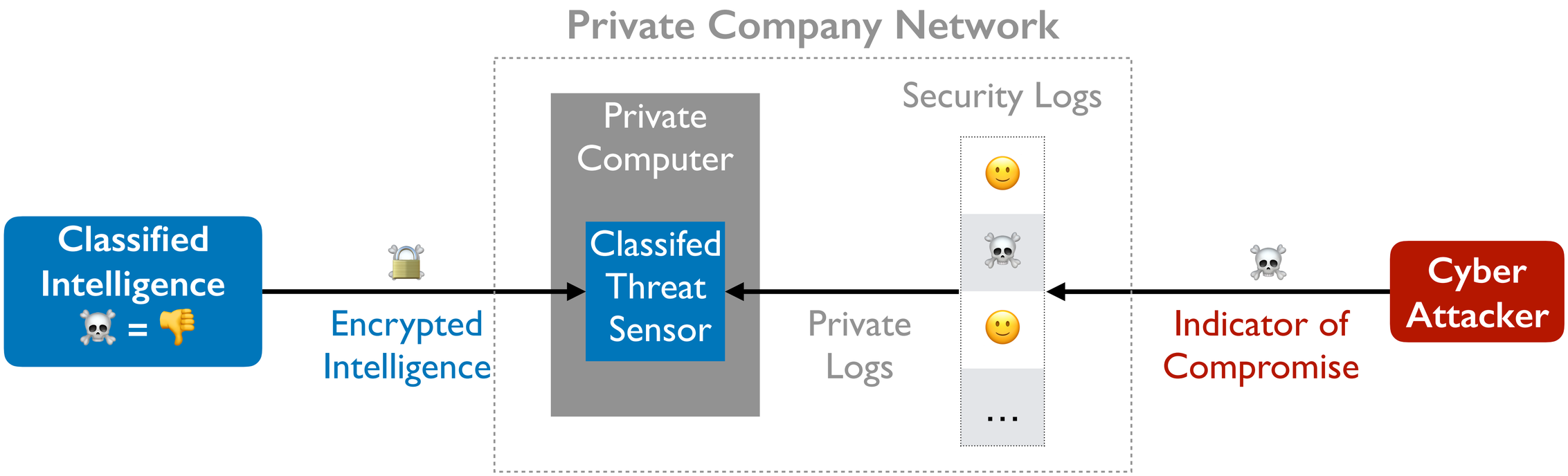
The Information Sharing Challenge

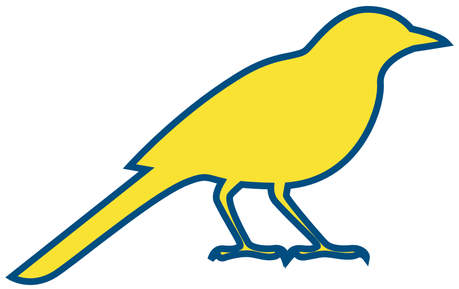


Can private industry apply classified intelligence without leaking it?

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

Classified Threat Sensors

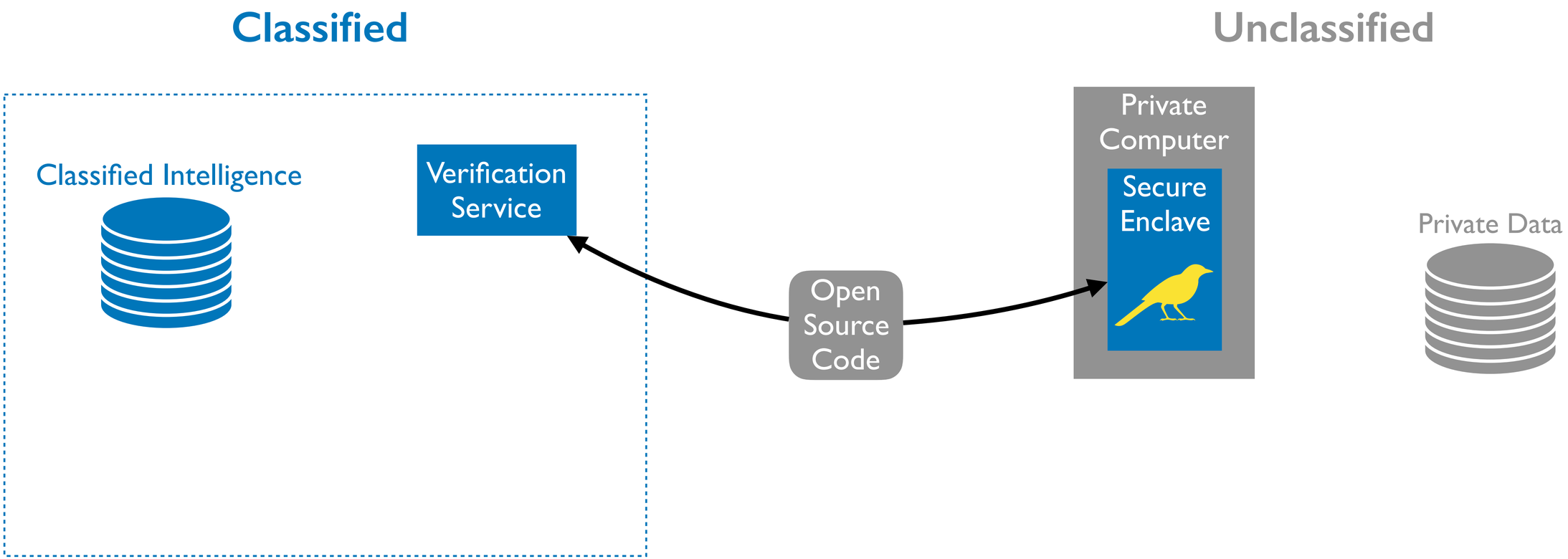




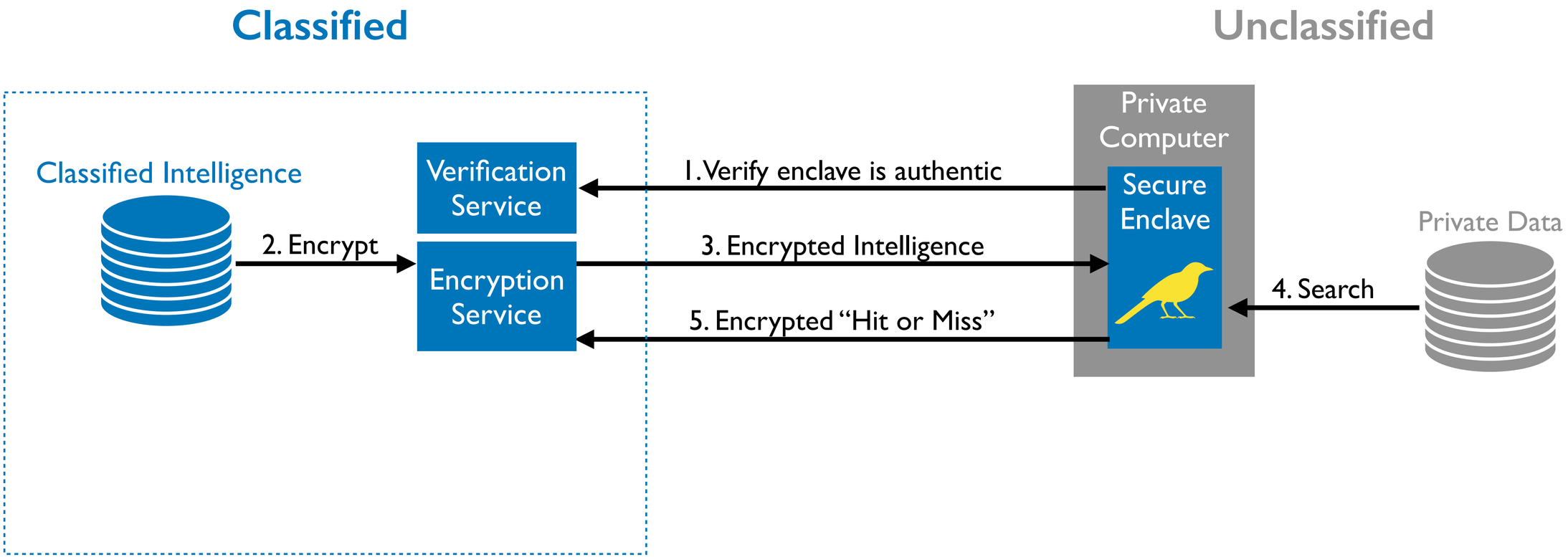
CANAREE: Classified Analysis of Network Attacks in a Restricted Execution Environment

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

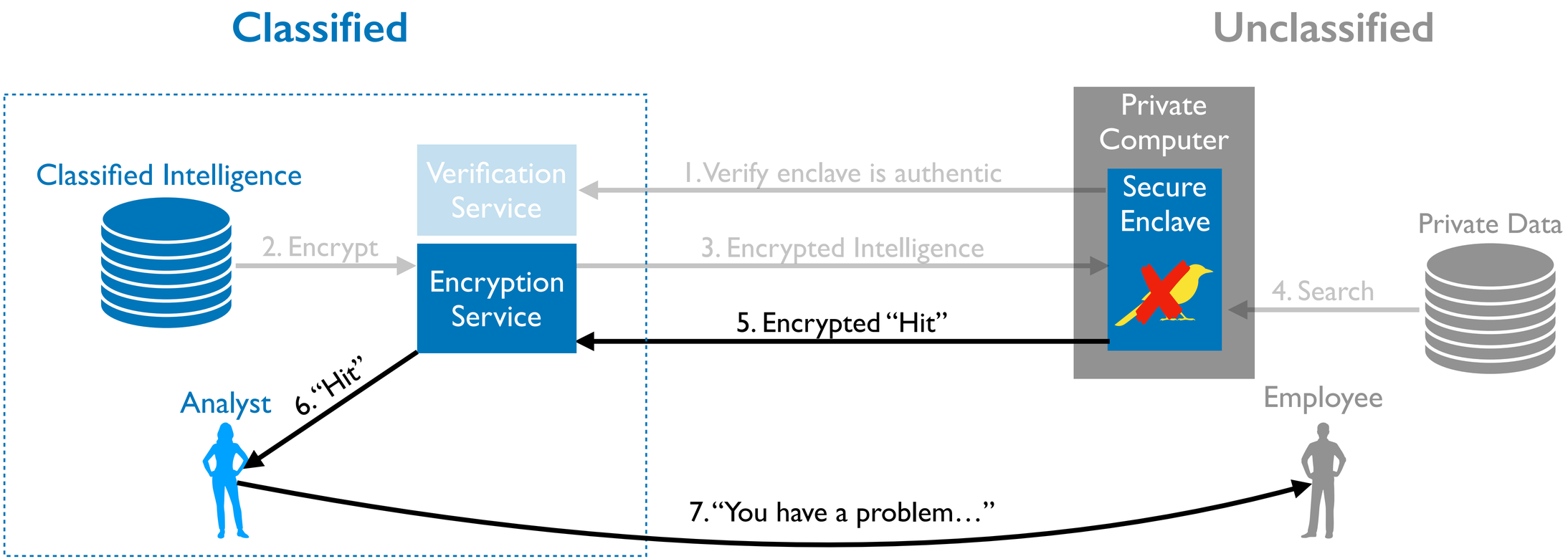
Starting a Classified Threat Sensor

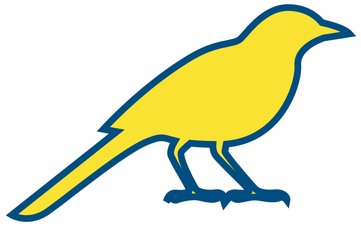


Searching for Threats in Private Data

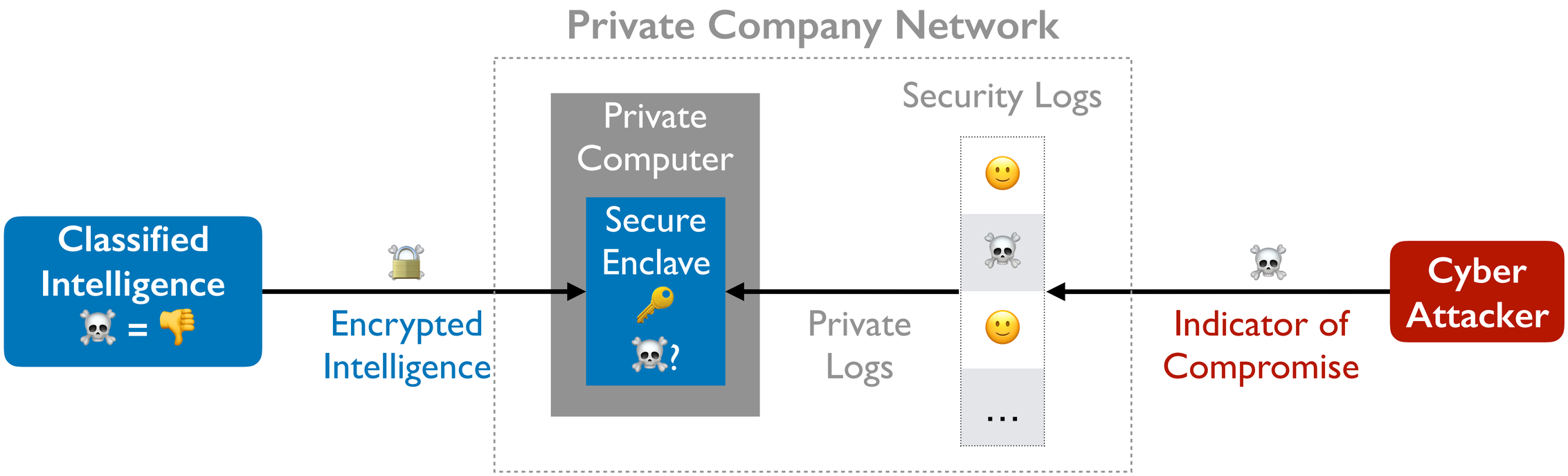


Responding to Detected Threats





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



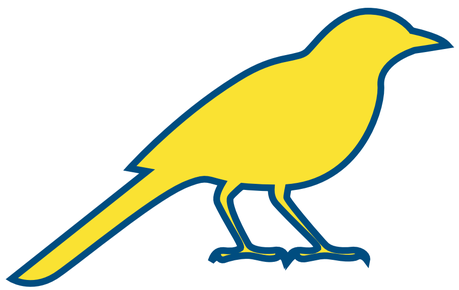
Five Phase Plan

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

Call for Funding

- Call for **$150,000 grant** to develop a classified threat sensor.
- Funding will cover **2 student developers for 1 semester** plus a part time PI.
- Working prototype should be delivered in **6 months.**
- All software will be available under **open source license**.

Thanks to Generous Supporters



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

For more information, please visit:
https://saweis.net/canaree