Probity | SIGNED EXECUTION EVIDENCE

Logs can be rewritten. Signatures cannot.

Connect
in/sankalp-gilda

The full story
beta · standard

When an agent escapes its sandbox, **"trust our logs"** isn't evidence — it's a press release.
We run untrusted agent code in a locked box and sign a receipt of exactly what it did.

WHAT A BREACH LEAVES BEHIND

incident.log — reconstructed

```
03:14:23 net.egress ALLOW host=cache:8080
03:14:41 … gap in record 03:14 → 03:20 …
03:1?:?? entry edited: "no anomalies"
03:19:57 net.egress host=huggingface.co (?)
03:20:01 fs.read /root/.cache/hf/token
09:02:00 [post-hoc] "contained." — vendor statement
```

hash — signature — verifier — UNVERIFIABLE

THE SIGNED RECEIPT WE EMIT

VERIFIED ed25519

```
event egress → huggingface.co
runtime sealed microVM · host-signed
sha256 a7f9c2e4…d1b3
sig 9e4d0af1…7c0b
chain tamper-evident · seq 41/41
```

$ **cosign verify-blob** --key probity.pub OFFLINE · NO VENDOR TRUST

Scanners read the code. **We run it — and sign the evidence.**