DETCORDON

CONTAINMENT & EVIDENCE / TEASER

Assume the guest is already lost.

01 / THE BOUNDARY

Trust less code.

The guest can become the adversary. The machinery around it must stay smaller, duller and harder to misuse.

~60k

security-critical user-space LOC

Firecracker + DetCordon runtime

OUTSIDE TRUST

Guest workload + guest kernel

payload / webshell / exploit chain / persistence attempts

FIRECRACKER v1.16.1 / ~50k LOC

jailer -> VMM -> vCPU threads

KVM / seccomp / cgroups / namespaces / chroot / minimal VirtIO

DETCORDON-OWNED RUNTIME

tap / supervisor / extractor / sink / guard

The compromised guest does not get to name the truth.

OBSERVE

DetectionOnly HTTP tap records bounded metadata; eBPF can add exec, write and connect telemetry.

CAPTURE

Extractor sends candidate file bodies outward. The guest cannot query the sink for them later.

RECOMPUTE

Sink computes SHA-256 itself. A hostile sender cannot simply declare a sample identity.

SEAL

Samples are age-encrypted to the analyst public key and stored by digest; sink writes are observed.

SHA-256

content identity computed at receiver

age

sink stores ciphertext; private key elsewhere

SSHSIG

canonical manifest verified offline

mTLS

producer certificate binds to source identity

Context can change. Evidence must not.

EVIDENCE / PRESERVED

What the run produced

Redacted events, encrypted sample artifacts, timestamps, source identity, configuration digests, custody lineage, checksums and detached signature.

- events.jsonl
- samples/<sha256>
- manifest.json
- checksums.txt
- bundle.sig

ENRICHMENT / DERIVED

What helps the analyst decide

ASN/network context, reputation, YARA/AV results, clustering, threat-intelligence matches, analyst annotations and machine summaries.

- replaceable
- time-sensitive
- source-attributed
- linked by digest
- never rewrites observation

Enrichment may be wrong and still be useful.

It must never be allowed to become the original.

04 / EVIDENCE REACHES A HUMAN

Every handoff is another chance to verify.

01

Sandbox -> sink

separate host / default-drop guest egress / distinct event/sample channels / reliable paths can use CA-validated TLS

02

Sink -> evidence bundle

sink-computed digests / age ciphertext / canonical manifest / custody fields / checksums / detached SSHSIG

03

Bundle -> archive / analyst

offline verification / archive copy verified again / signer trust anchor arrives through a separate channel