VCRI
THE VALUE CHAIN RISK INSTITUTE

VCRI LEARN · HOW VCRI WORKS

How the Beacon Collector works

From a vendor’s own tools to a score a buyer can check, without the evidence ever leaving the vendor’s machines.

Joshua Marpet and Cairn Viktor

VCRI
THE VALUE CHAIN RISK INSTITUTE

WHY DO I CARE

One idea, three audiences

A questionnaire tells you what a vendor says. Evidence tells you what its systems say.

If you buy

You get a score built from what a vendor's systems recorded, and a fingerprint that lets you check it.

Not another questionnaire answer.

If you sell

Show your posture from the tools you already run.

Your scan data and exports stay on your own machines.

If you are learning

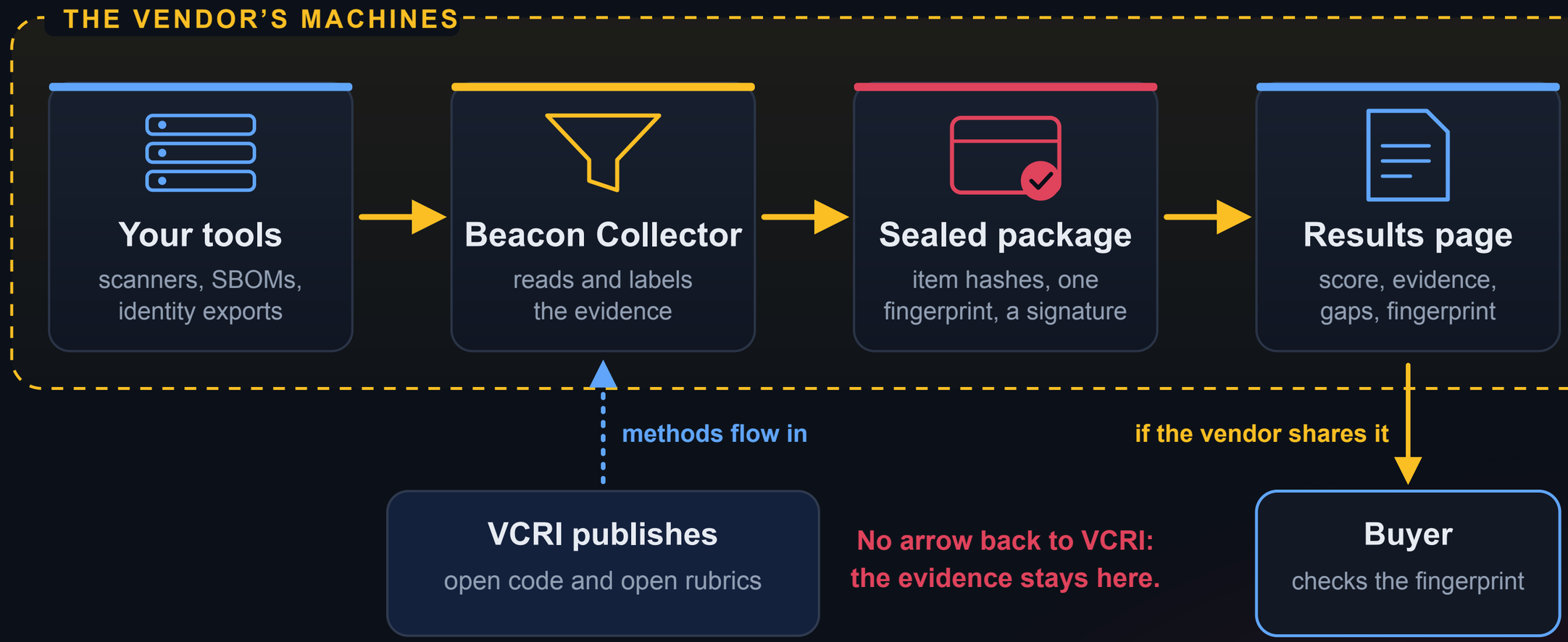
A working, open-source example of hashing, digital signatures and open scoring.

You can read every line.

valuechainrisk.org/learn · CC BY 4.0

THE WHOLE PICTURE

Evidence stays put. Methods flow in.



valuechainrisk.org/learn · CC BY 4.0

VCRI
THE VALUE CHAIN RISK INSTITUTE

STEP 1

What a vendor runs

Observe, never alter: in the container it reads your disk read-only, opens no network ports, and only connects outward.

Install
On a machine that can reach your tools. Python, or a signed container.

→

Point it
At what you already have: a scan, an export, an SBOM, your AI agents' configuration.

→

Seal
The collector writes the evidence package and its fingerprint.

→

Open results
A page in your browser: the score, the evidence, the gaps.

valuechainrisk.org/learn · CC BY 4.0

STEP 2

What evidence it reads

Systems

Vulnerability scanner results.

Email and TLS settings on your own domain.

Software

SBOMs, and OpenSSF Scorecard results for open-source projects.

OSCAL documents (a machine-readable compliance format).

People and access

Identity-provider exports: who has accounts, and MFA.

Training and phishing-simulation records.

AI agents

Every model, plugin, MCP server, prompt and memory store an agent depends on, as an AI bill of materials.

valuechainrisk.org/learn · CC BY 4.0

VCRI
THE VALUE CHAIN RISK INSTITUTE

STEP 2, CONTINUED

Not all evidence is equal

Each item is labeled by how strong it is. The label sets the highest maturity level it can earn, on a 1 to 5 scale.

4

Observed

A tool saw it on the system, like a scanner result.

3

Recorded

A system wrote it at the time, like training completions.

2

Attested

A third party's report, like an audit, sealed as is.

1

Stated

The vendor's own claim, sealed but unverified.

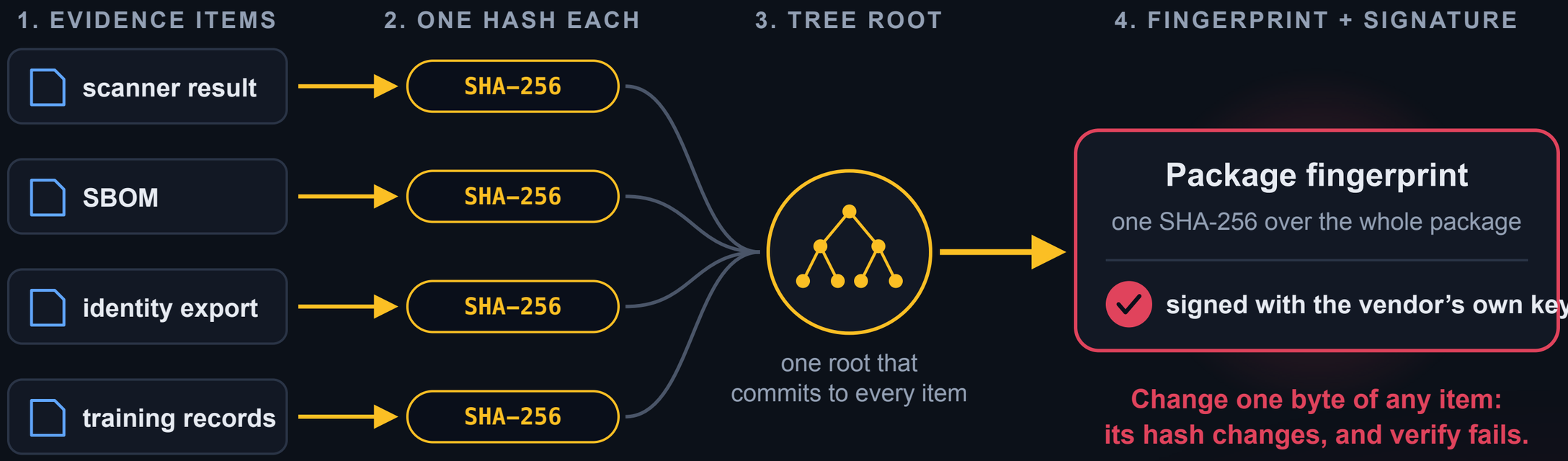
Level 5 is never awarded by the free scorer.

valuechainrisk.org/learn · CC BY 4.0

VCRI
THE VALUE CHAIN RISK INSTITUTE

STEP 3

The sealed evidence package



valuechainrisk.org/learn · CC BY 4.0

VCRI
THE VALUE CHAIN RISK INSTITUTE

STEP 4

Scored against open rubrics

Verify first

A package that fails verification gets no score.

Its results page says REFUSED.

Open arithmetic

Published rubrics, one per PPTDF-AI asset class: People, Processes, Technology, Data, Facilities, AI.

Same math as the BeaconScore questionnaire.

Two numbers, always together

Comparable: missing evidence counts as zero.

Covered: scored over the evidence present, with the coverage percentage.

Nothing averaged away

When observed and attested evidence disagree, the page shows the contradiction.

Evidence with no place in a rubric is listed as a gap.

Beta scores use a draft method and are labeled that way on the page.

valuechainrisk.org/learn · CC BY 4.0

VCRI
THE VALUE CHAIN RISK INSTITUTE

STEP 5

What a buyer sees

ON THE RESULTS PAGE	WHAT IT TELLS THE BUYER
Verified or REFUSED	Whether the seal held. A broken package shows no score.
Package fingerprint	The exact package this page was built from.
Grade and score per rubric	Where the vendor stands, area by area.
The evidence behind every number	Which item, and which class, produced each level.
Contradictions and gaps	Where sources disagree, and what is missing.

The page says it is “a position on the evidence, not a certification.”

valuechainrisk.org/learn · CC BY 4.0

VCRI
THE VALUE CHAIN RISK INSTITUTE

THE DESIGN CHOICE

Why the evidence never leaves

Nothing to hand over

VCRI never holds vendor evidence.

No central pile of every vendor's scan results to collect, store or lose.

Trust the math, not the custodian

The fingerprint and signature make any copy checkable, so nobody has to take a holder's word for it.

Show one item, not all

The package format can prove one item is inside the seal without revealing the others.

Coming later

Public timestamps on the fingerprint, so buyers you choose can confirm a score and when it was made, without a questionnaire.

valuechainrisk.org/learn · CC BY 4.0

VCRI
THE VALUE CHAIN RISK INSTITUTE

WHAT TO DO MONDAY

Try it, then break it

- Sign up for the Beacon beta at valuechainrisk.org/beta.
- Seal one thing you already have: an SBOM or a scanner result. Open the results page.
- Change one byte of the package and run verify again. Watch it fail.
- Buying? Next time, ask a vendor for evidence and a fingerprint, not another form.
- Take the two-minute Security Tools Poll at valuechainrisk.org/tools-poll, so the collector learns your tools first.

valuechainrisk.org/learn · CC BY 4.0

VCRI

THE VALUE CHAIN
RISK INSTITUTE

Free to use, teach and share.

This deck is part of the VCRI Learn series. Use it in your class, your team meeting or your chapter, with credit to The Value Chain Risk Institute.

valuechainrisk.org/learn

valuechainrisk.org/learn · CC BY 4.0