OSCRAT

Open-Source Cyber Resilience Act Tools

Follow us on social media

Co-funded by
the European Union

ECCC
EUROPEAN CYBERSECURITY
COMPETENCE CENTRE

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. – Project: 101190180

Embedding Risk Management into the Development Lifecycle

CRA-focused case study using vulnerability scan results

Yasen Tanev

Co-funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE
OSCRAT

CRA Changes the Game

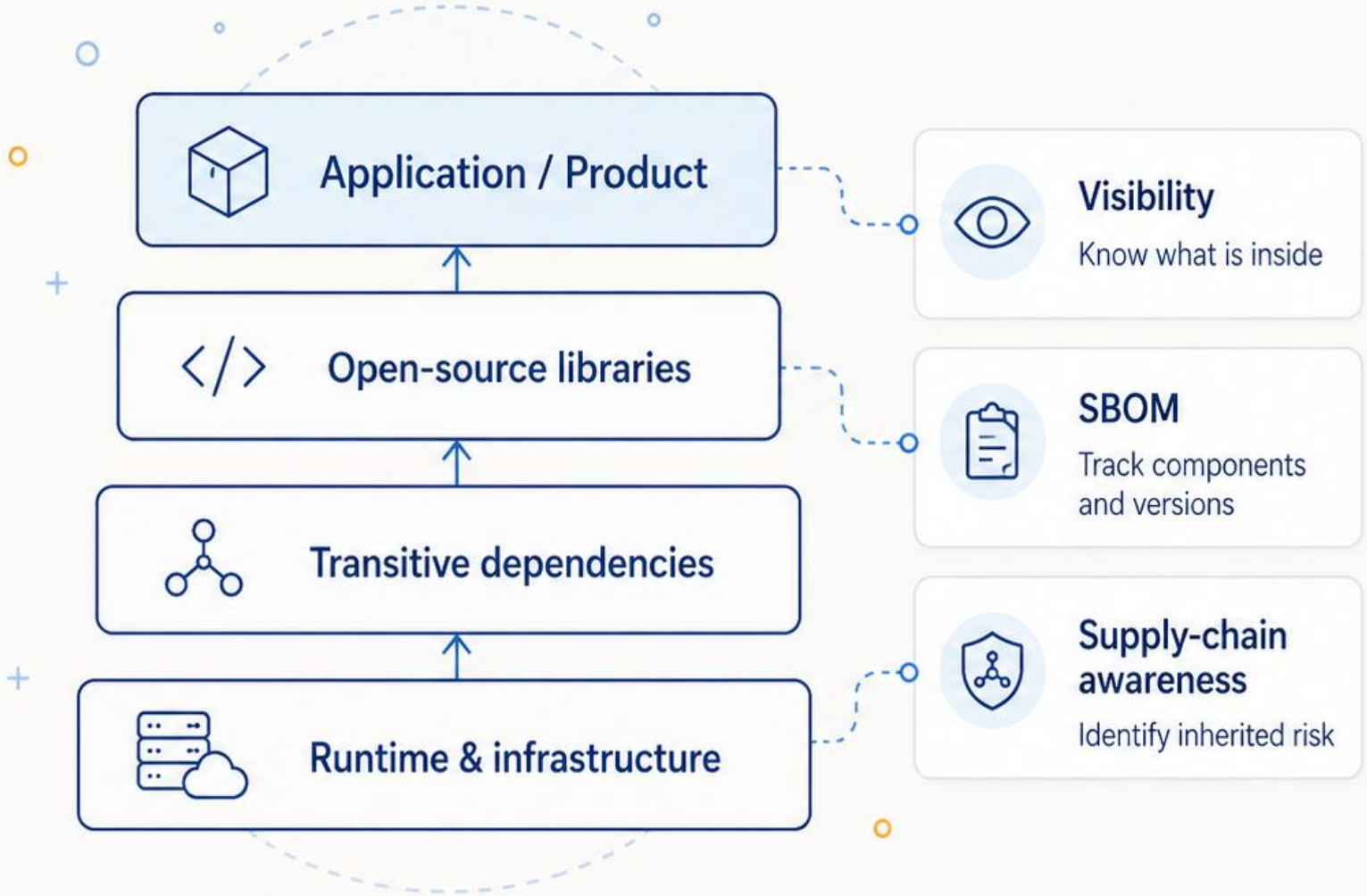
From best practice to legal obligation

- Applies to products with digital elements
- Security by design and by default
- Cybersecurity across the full lifecycle
- Compliance must be demonstrable

Co-funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE
OSCRAT

Where Product Risk Comes From

Component risk becomes product risk



Co-funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE
OSCRAT

Real Vulnerability Scan Example

Example product: stardust-fine-edition 1.0

Component	Version	Key findings	Severity
log4j-core	2.14.1	RCE, Log4Shell chain	Critical
lodash	4.17.20	Injection, pollution, ReDoS	High / Medium

Severity legend

- Critical
- High
- Medium

These findings become CRA risk objects for assessment and treatment.

Co-funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE
OSCRAT

From Vulnerability to CRA Risk

A scan is an input, not the end of the process

CRA expects risks to be identified, treated, and evidenced across the product lifecycle.

Co-funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE
OSCRAT

Risk Register: Core Compliance Artifact

The central place to manage product cybersecurity risk

- Single source of truth for identified risks
- Supports technical documentation and audit readiness
- Tracks owner, status, treatment, and evidence

What it should contain

- Risk ID
- Component
- Vulnerability
- Impact
- Treatment
- Owner
- Status
- Evidence

Without a structured register, traceability is weak.

Co-funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE
OSCRAT

Example Risk Register Entries

Derived from the vulnerability scan

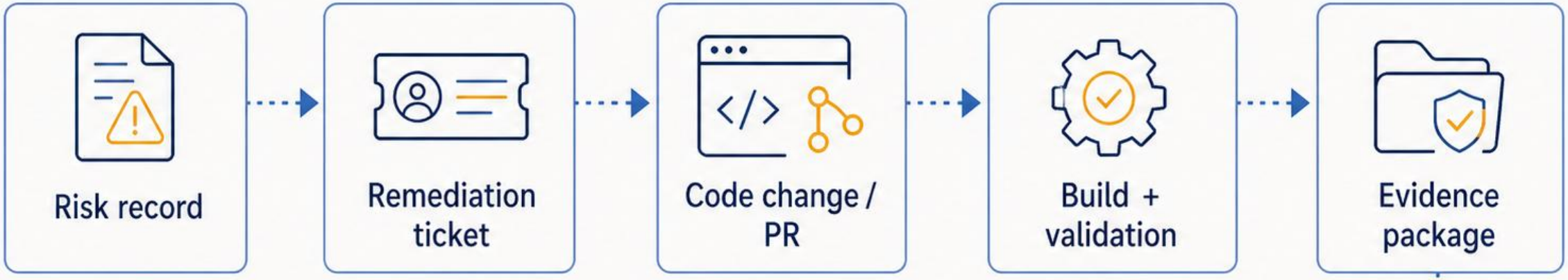
Risk ID	Component	Risk	Treatment	Status
R-001	log4j-core 2.14.1	CVE-2021-44228 • Critical RCE	Upgrade to 2.17.1+	Open
R-002	lodash 4.17.20	CVE-2021-23337 • High injection	Upgrade to 4.17.21+	Open
R-003	lodash 4.17.20	CVE-2025-13465 • Prototype pollution	Upgrade to 4.17.23+	Open

Next step: assign owner, create task, attach evidence.

Co-funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE
OSCRAT

Traceability: Risk → Task → Evidence

This is how compliance becomes provable



Auditors look for the link between **finding**, **action**, and **proof**.

Co-funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE
OSCRAT

Practical Risk Treatment

Common options for handling product cyber risk

1 **Mitigate**

- Patch / upgrade
- Add security controls

2 **Avoid**

- Remove risky component
- Change design

3 **Accept**

- Residual risk justified
- Document decision

4 **Monitor**

- Track exposure
- Watch for fix or exploit

Acceptance should be explicit, limited, and evidence-based.

Co-funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE
OSCRAT

Using Risk to Support Decisions

Risk management helps decide what happens next

Scenario:
critical vulnerability found before release

Can we release?

- Patch before release
- Release with justified residual risk
- Hold release and redesign

Backlog priority

Release approval

Resource allocation

Stakeholder communication

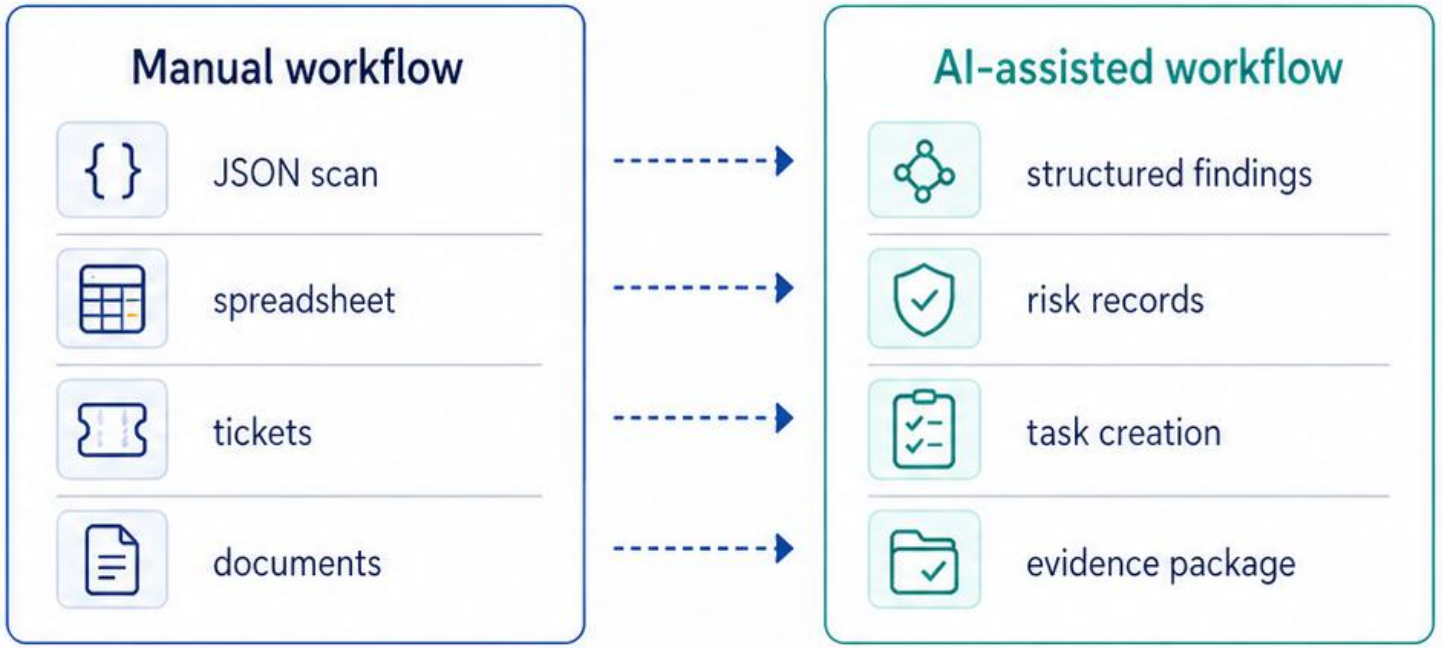
Risk is a decision support mechanism, not just a register.

Co-funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE
OSCRAT

Why AI Matters for CRA Workflows

Turning raw security findings into structured compliance actions

- Too many findings to triage manually
- Fragmented data across tools
- Manual documentation is slow
- Traceability is hard to maintain at scale

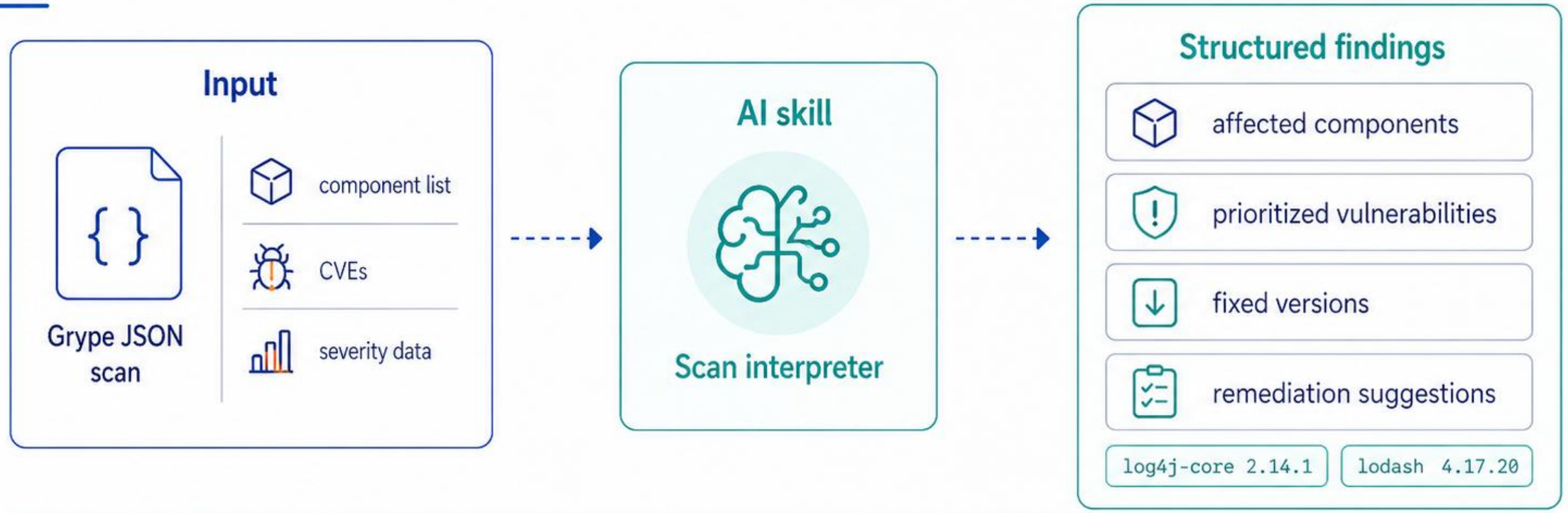


AI improves speed, consistency, and scalability — while accountability remains human.

Co-funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE
OSCRAT

Skill 1: Vulnerability Scan Interpreter

From raw scan output to structured technical findings

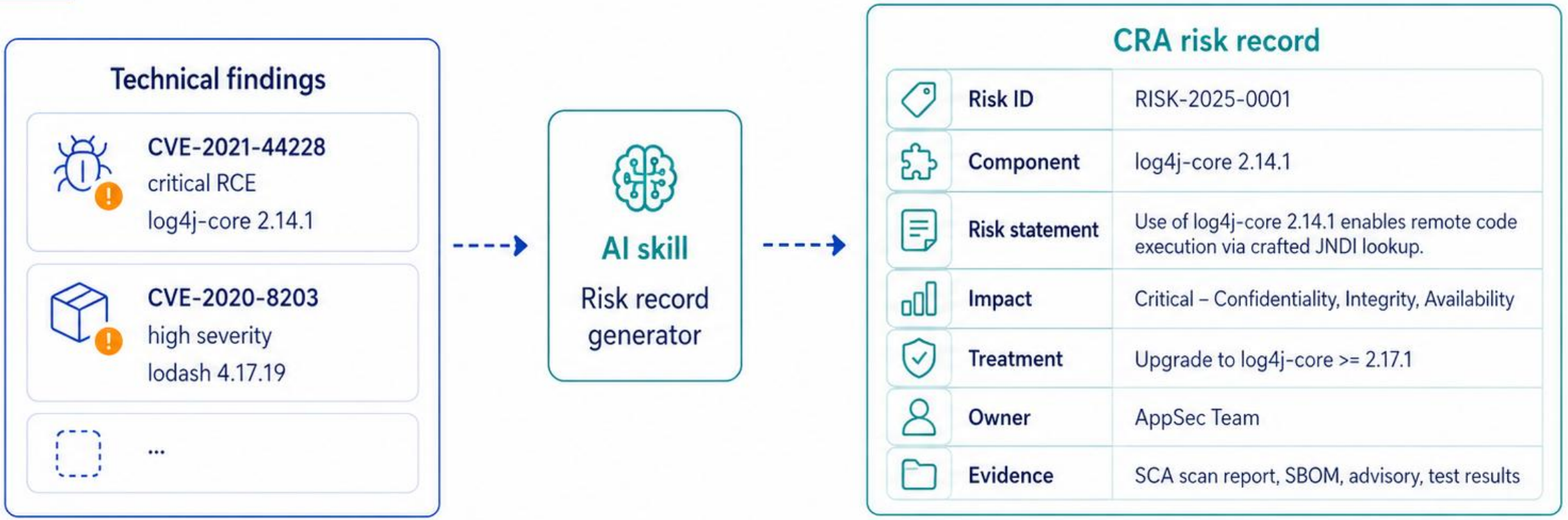


Use case: turn raw scan files into CRA-ready technical summaries.

Co-funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE
OSCRAT

Skill 2: CRA Risk Register Generator

Transforming technical findings into compliance-ready risk records

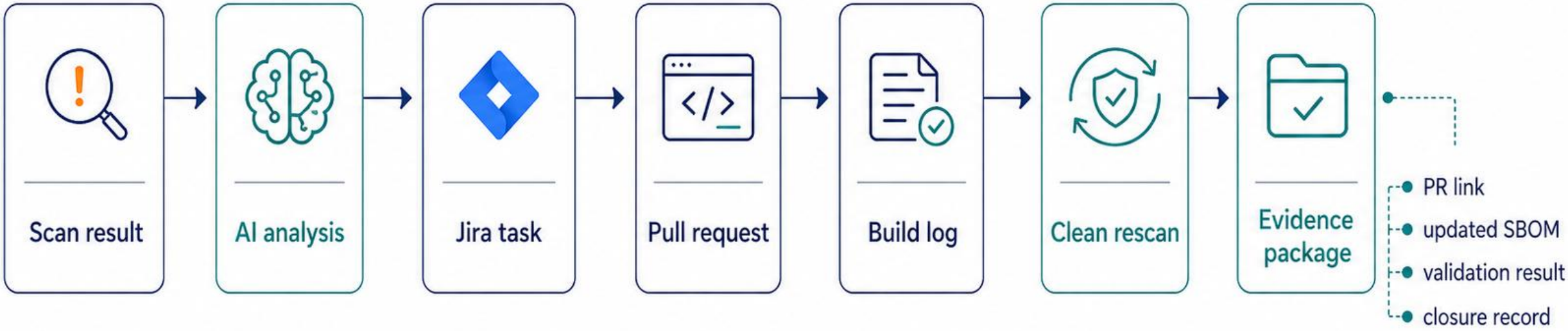


AI standardizes risk language and reduces documentation effort.

Co-funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE
OSCRAT

Skill 3: Traceability & Evidence Builder

Linking findings, actions, and proof across the lifecycle



This makes CRA traceability scalable and audit-ready.

Co-funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE
OSCRAT

AI as a Practical CRA Enabler

Helping teams interpret, structure, connect, and prove

Interpret findings

understand raw scan data

Structure risk

generate compliance-ready records

Connect tasks

link work across tools

Prove evidence

support audit readiness

It is not enough to fix vulnerabilities — organizations must prove they managed the risk.

AI helps teams move from scan results to provable CRA compliance.

Co-funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE
OSCRAT

16. What We Are Doing with This Skill

Co-funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE
OSCRAT

End-to-end CRA-aligned risk management from SBOM to report with guided gap analysis.

HOW THE SKILL HELPS

Knows Where You Are
Identifies the current stage (0–6) of the risk assessment based on available data.

Finds Gaps
Analyzes what is missing and asks targeted questions to close the gaps.

Turns Data into Risk
Converts scan findings into clear risk statements and risk register entries.

Drives Mitigation
Recommends treatments, creates actionable tasks and tracks remediation.

Ensures Traceability
Maps risks to tasks, evidence and decisions for audit readiness.

Delivers Reports
Produces executive and technical reports aligned with CRA expectations.

Outcome: A structured, repeatable, and auditable process that reduces cybersecurity risk, supports CRA obligations, and builds trust in the products we deliver.

We help you:

- Understand your risk posture
- Prioritize what matters most
- Take the right actions
- Prove it with evidence
- Make informed release decisions

OSCRAT

Open-Source Cyber Resilience Act Tools

Follow us on social media

Co-funded by the European Union

ECCC

EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. – Project: 101190180