CYBER RESILIENCE PLATFORM

SECURE BY EVIDENCE

TECHNICAL CAPABILITIES / CONFIDENTIAL DRAFT

# AA-sec: Capabilities & Security

Automate CRA compliance. Keep control. Prove every step.

WHO WE ARE

# Built for Engineering and quality-led delivery

## Anton C.

QA Lead
Process Automation
MCP guru

## Anton V.

Critical-safety systems architect
Cybersecurity specialist
Embedded engineer

**Why trust us:** Critical-safety engineering discipline. QA-grade repeatability. Evidence by design. Built by practitioners, for practitioners.

THE PROBLEM

# Evidence Should Not Live in Spreadsheets

## Current State

Evidence is typically distributed across existing tools, repositories, tickets, and documentation. Preparing a complete compliance view often requires teams to bring these sources together manually

## Target State

Fully automate CRA compliance evidence through simple integrations, built-in scanning, and ready workflows. Product teams keep audit-ready proof current. Without building their own compliance platform.

PLATFORM OVERVIEW

# One Platform for the Full CRA Product Lifecycle

Manage the product, automate compliance, monitor what changes, and keep the evidence ready.

### Organization & Access

Users, roles, permissions

### Products & Releases

Products, sub-products, versions

### CRA Assessment

Requirements and compliance lifecycle

### SBOM & Vulnerabilities

Components, vulnerability sources, processing

### Post-Market & Article 14

Continuous monitoring and regulatory workflows

### Evidence & Traceability

Evidence, provenance, activity history

### Document Automation

Templates, dossiers, generated documents

### Integrations

Standard APIs and custom integrations

### Security by Design

Data Isolation · Cryptography · Decentralized Recovery

ORGANIZATION & ACCESS

# Organize Teams. Control Access.

Set up your organization, define responsibilities, and control who can access what.

## Organization Management

Create and manage organization information and structure.

## Users & Teams

Add users and organize the people working with your products.

## Roles & Permissions

Assign responsibilities and define what each role is allowed to do.

## Controlled Visibility

Ensure users only see the products and information available to them.

PRODUCTS & RELEASES

# Model Products. Manage Every Release.

Structure products and sub-products, manage versions and releases, and keep their lifecycle organized in one place.

## Product Structure

Create and manage products as the foundation of their CRA lifecycle.

## Sub-products

Model complex products through connected sub-products and components.

## Versions

Track product evolution across multiple versions.

## Releases

Create and manage releases with their own product and compliance context.

LIFECYCLE MODEL

# Product & Release Model: Lifecycle is Ready

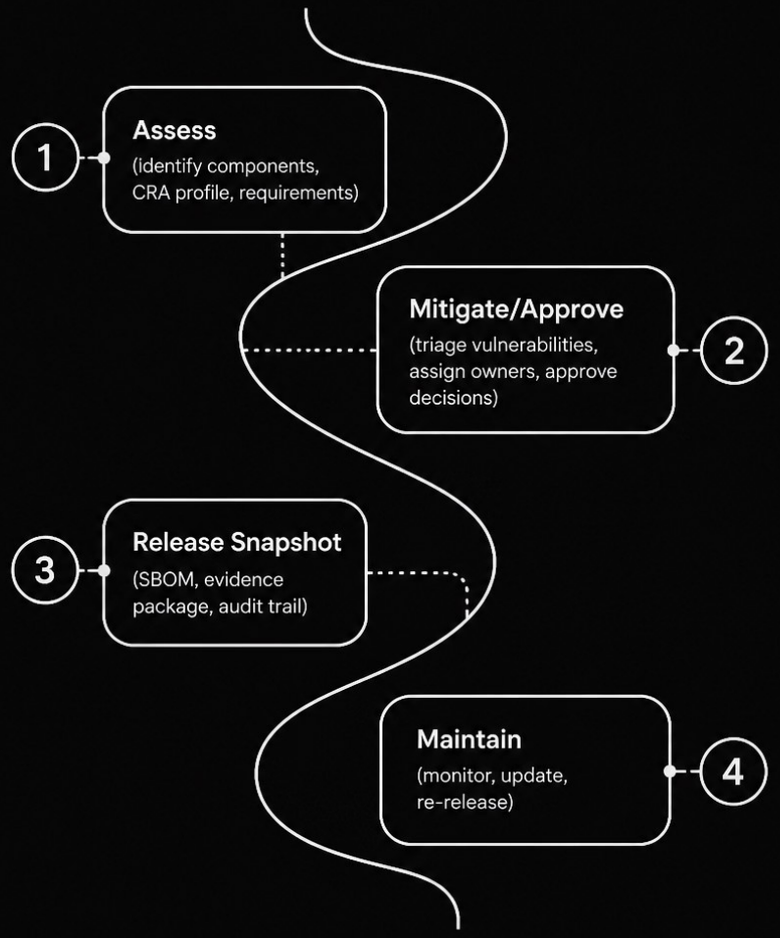
## Product = Living Context

Product identity, owners, components, requirements, CRA profile, intended use, lifecycle responsibilities, and organizational accountability — continuously maintained.

---

## Release = Reviewable Snapshot

A specific version boundary with SBOM snapshot, vulnerability state, decisions, evidence package, generated documents, and full audit trail.



CRA ASSESSMENT

# Assess Requirements. Track Compliance.

Turn CRA requirements into a structured assessment process and keep the compliance state of every product visible.

## Applicable Requirements

Work with the CRA requirements relevant to each product.

## Structured Assessment

Evaluate requirements through a consistent and repeatable workflow.

## Compliance Status

See what is complete, what needs attention, and where evidence is still required.

## Continuous Lifecycle

Keep assessments aligned as products, versions, and compliance data evolve.

SBOM & VULNERABILITIES

# Know What You Ship.
# Know What Is Vulnerable.

Turn SBOM data into structured component intelligence and continuously evaluate it against connected vulnerability sources.

---

### SBOM Processing

Import and process SBOMs as part of the product lifecycle.

### Component Intelligence

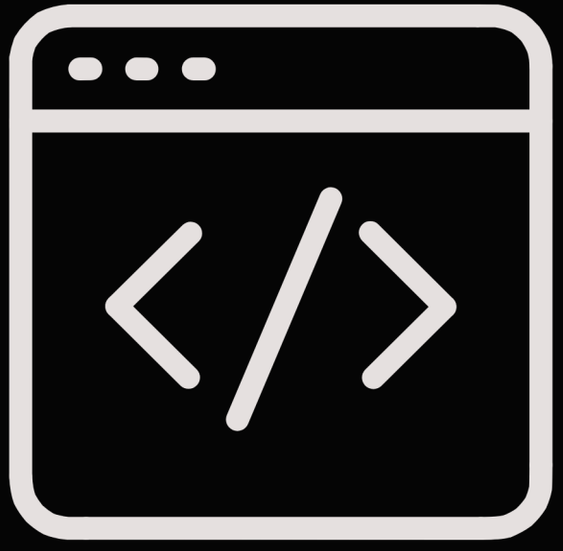
Identify and manage the software components behind each product and release.

### Vulnerability Analysis

Match components against vulnerability data and track relevant findings.

### Extensible Sources

Connect multiple vulnerability databases and add new sources as they become available.



SBOM & SCANNER

# Built-in Scanner and SBOM Pipeline


AA-sec treats SBOM as a first-class product-security object. External CI/CD scanners, SBOM exporters, and vulnerability sources can feed the platform through normalizers — but AA-sec owns the normalized security state and evidence trail.

POST-MARKET & ARTICLE 14

# Monitor After Release. React on Time.

Keep released products under continuous watch and turn relevant security events into structured CRA Article 14 workflows.

### Continuous Monitoring

Keep released products and their known components under ongoing vulnerability monitoring.

### Relevant Changes

Detect when new vulnerability information becomes relevant to an existing product or release.

### Article 14 Workflows

Guide required actions and reporting through a structured regulatory workflow.

### Alerts & Deadlines

Notify responsible users and keep critical Article 14 deadlines visible and actionable.

ARTICLE 14

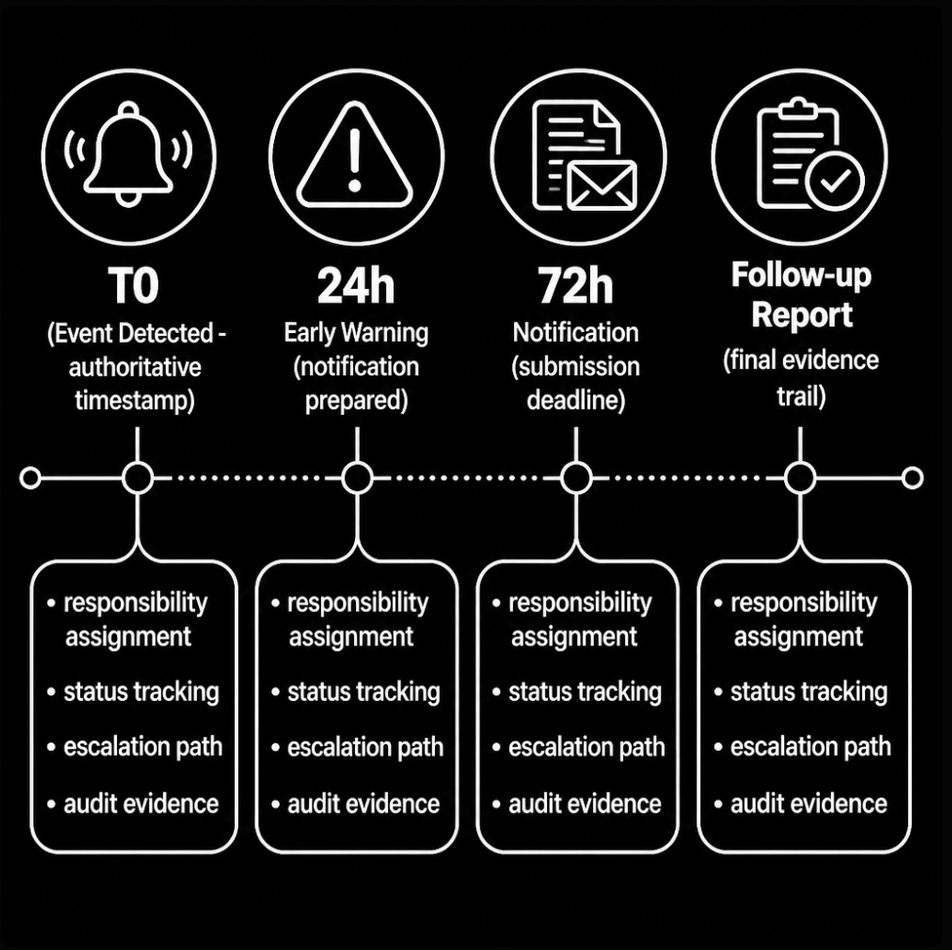
# CRA Article 14 Workflow Engine

Deadline logic is persisted as state and derived timestamps — not fragile in-memory timers.
Restart or deployment does not erase compliance obligations.

Operational Flow

- **T0:** Event detected — authoritative timestamp created
- **24h:** Early warning window triggered
- **72h:** Notification deadline enforced
- **Follow-up:** Final report window tracked

Scheduled checks query persisted deadlines and workflow state. Responsibility, status, blockers, escalation paths, and submission evidence are all recorded.



EVIDENCE & TRACEABILITY

# Keep the Proof.
# Trace Every Change.

Build a living evidence base around every product — connected to its requirements, releases, assessments, and history.

## Evidence Base

Collect and manage the information and artifacts that support product compliance.

## Connected Evidence

Link evidence to the relevant products, releases, requirements, and assessments.

## Provenance

Preserve where evidence came from and the context in which it was created.

## Activity History

Keep a traceable record of important actions and changes across the product lifecycle.

DOCUMENT AUTOMATION

# Generate Documents from Live Compliance Data.

Turn product data and evidence into consistent, traceable documents using flexible and configurable templates.

AA-sec forms documents from existing evidence, allows you to customize their content and appearance, and maintains the connection between the result and the source data.

## Automated Generation

Generate compliance documents and dossiers directly from platform data.

## Flexible Templates

Configure document structure and content for different organizational needs.

## Custom Appearance

Adapt branding, layout, and presentation without changing the underlying compliance data.

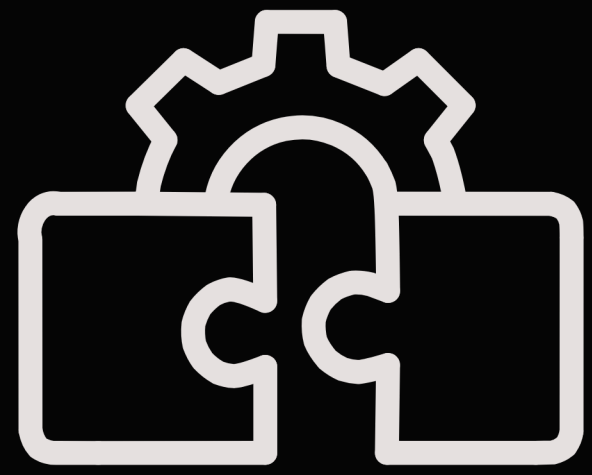
## Verifiable Provenance

Keep generated content connected to the source data and evidence behind it.

INTEGRATIONS & AUTOMATION

# Connect Your Toolchain. Automate the Workflow.

Bring compliance into the tools and processes your teams already use — through standard integrations, APIs, and custom connections.



## Standard Integrations

Connect common engineering and security tools to exchange relevant product and compliance data.

## API Access

Automate platform capabilities directly from existing workflows and systems.

## Custom Integrations

Extend connectivity for organization-specific tools and processes.

## Workflow Automation

Reduce manual handovers by moving data and actions between AA-sec and the surrounding toolchain.

CRYPTOGRAPHY & RECOVERY

# Encrypt by Design.
# Recover Without a Single Point of Trust.

Protect organizational data with built-in cryptography
while keeping recovery decentralized and under controlled trust.

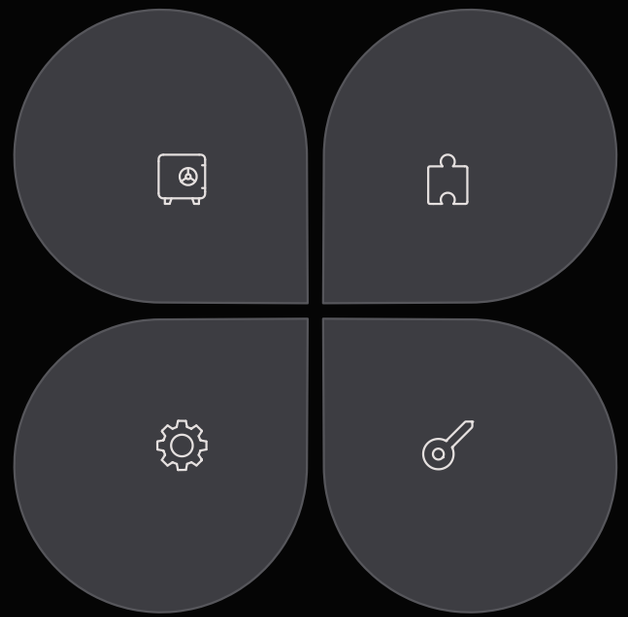
---

## Organization-Scoped Encryption

Protect sensitive platform data within the cryptographic context of each organization.

## Built Into the Platform

Encryption and recovery are part of the platform design, not optional layers added around the data.



## Separated Trust

Keep cryptographic access boundaries separated instead of relying on one universal trust point.

## Decentralized Recovery

Recover access through a distributed recovery model rather than a single master recovery secret.

WORKFLOW FLEXIBILITY

UI

# The UI

Use the interface to manage products, assessments, evidence, and documents in one place.

### Guided Workflows

Use structured platform workflows for day-to-day compliance work.

### Direct Visibility

See products, assessments, evidence, and status in one interface.

### Team Collaboration

Work across roles with shared visibility and controlled access.

### No Extra Tooling Required

Start working immediately without building custom automation first.

API

# Or the API

Use the API to integrate AA-sec into existing engineering, security, and compliance processes.

### Automation-Ready

Trigger platform actions directly from your existing systems and pipelines.

### System Integration

Exchange data with external tools and internal workflows.

### Custom Processes

Adapt AA-sec to organization-specific processes and toolchains.

### Scale Through Automation

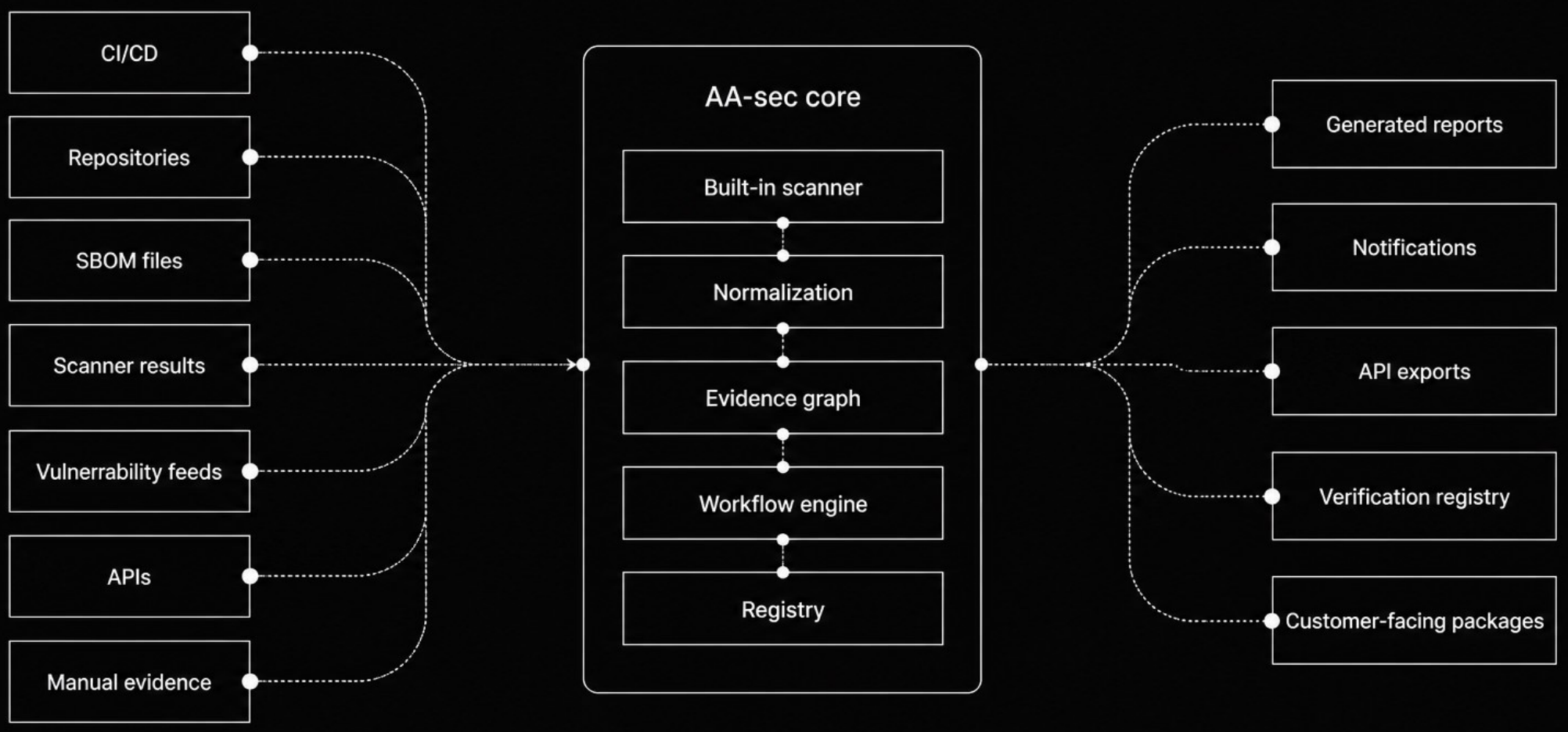
Reduce manual handovers and embed compliance into recurring workflows.

Use AA-sec through the interface, through the API, or through both together.

INTEGRATION

# Integration Architecture

AA-sec provides a flexible integration architecture, allowing seamless ingestion of diverse data sources, robust internal processing, and varied output distribution, adapting to your existing ecosystem.




## Operational Modes

### Scanner-First Mode

Clients without an existing Dependency-Track or scanner stack can leverage AA-sec to perform dependency and vulnerability scanning independently.

### Connector Mode

If a client already has a scanner or toolchain, it can be integrated as a data source, feeding AA-sec with existing security insights.

### Output-Only Automation

MCP/API consumers can retrieve results and evidence without becoming the owner of the compliance state, enabling downstream automation.

MCP

# Bring Your Own AI Agent.

Connect your AI agent to AA-sec through MCP and let it work with structured product, compliance, and evidence context.

Your AI Agent

MCP

AA-sec Platform

### Structured Context

Give your agent access to product, compliance, vulnerability, and evidence context in a machine-friendly form.

### Same Access Boundaries

The agent operates within the same organization and authorization boundaries as the rest of the platform.

### Use Your Own AI

Keep the choice of model, agent architecture, and surrounding AI workflow on your side.

**MCP exposes platform context to the agent.**

Data ingestion and platform writes remain on the standard integration/API path.

Self-hosted telemetry: opt-in only.

PRODUCT LIFECYCLE

# Compliance Does Not End at Release

AA-sec provides continuous oversight, integrating compliance directly into your product's entire journey, from inception through operation and subsequent iterations.

**Product**
Define and create

**Assess**
CRA, SBOM, vulnerabilities

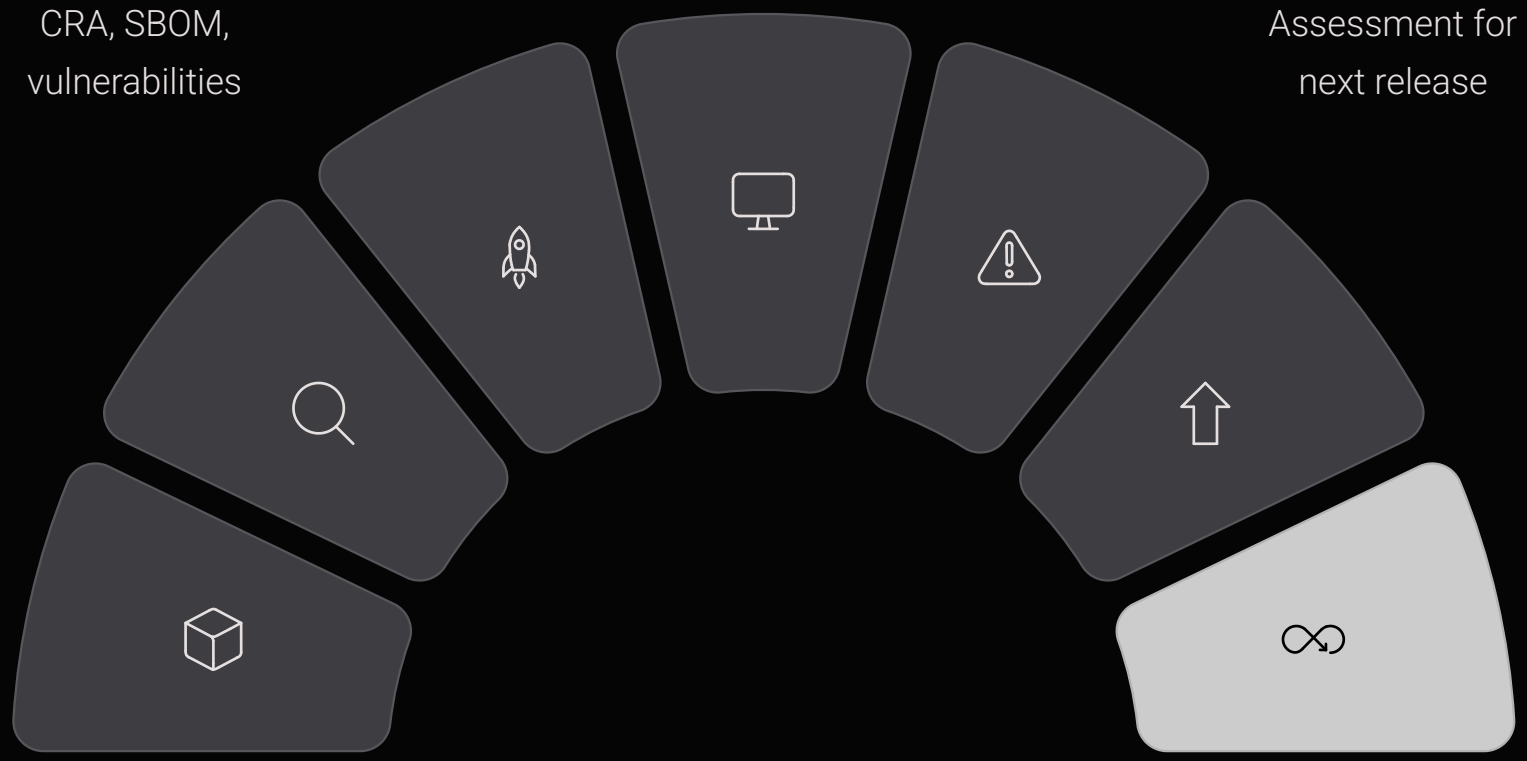
**Release**
Prepare and deploy

**Monitor**
Ongoing operational oversight

**React**
To changes and vulnerabilities

**Update**
Assessment for next release

**Repeat**
Even if in 10 years



Evidence accumulates throughout the lifecycle. Documents are generated from the current state.

What you did today will still be there tomorrow.

OPERATIONAL DESIGN

# Reliability and Operational Design

AA-sec is engineered for continuous availability and data integrity, ensuring that critical compliance evidence is always preserved and processes are resilient to disruptions.

## Persistent State

Compliance-critical data like deadlines, findings, workflow state, evidence, and artifacts are saved as durable records.

## Queue-Backed Work

Long-running operations (scanning, document generation, notifications) are processed asynchronously with built-in retry handling.

## Restart-Safe Mechanics

CRA Article 14 workflows and document generation are designed to be process-agnostic, not relying on long-lived sessions.

## Idempotent Processing

Re-running a job or operation will not create duplicate compliance events or records, ensuring data consistency.

## Operational Visibility

Comprehensive logs, health checks, status APIs, and audit events provide transparent insight into system operations and failures.

## Controlled Change

Database, schema, and release changes are managed to ensure they do not compromise or corrupt historical compliance data.

**Key Outcome:** Compliance obligations and evidence are designed to survive worker failures, service restarts, and delayed processing.

DEPLOYMENT

# Your Environment. Our Platform. Delivered Together.

For organizations with stringent infrastructure control and data residency requirements,

AA-sec offers a robust on-premise deployment package.

## Deploy in Your Environment

AA-sec can be packaged for installation within your customer-controlled infrastructure, providing complete ownership of the deployment and your data.

## Use Your Systems

We can integrate with your existing identity provider, storage solutions, security tooling, and internal operational processes.

## Start with Us

Our team provides expert guidance to configure, connect, validate, and onboard your initial compliance workflows for a seamless launch.

**Goal:** Make AA-sec fit your operating model — not force your teams to rebuild it.

DEPLOYMENT

# Deployment Model and Trust Boundaries

AA-sec offers flexible deployment options designed to meet varying customer requirements for control, compliance, and infrastructure isolation.

## AA-sec EU SaaS

READY

This is the primary offering, where AA-sec manages:

- Hosting
- Deployment
- Updates
- Operations

Infrastructure is hosted in the EU, ensuring data residency.

## Dedicated Deployment

PLANNED

A separate, dedicated customer environment for enhanced isolation.

Suitable for clients where procurement or security policies require greater infrastructural separation from multi-tenant environments.

We know how picky IT is.

## On-Premise Package

NOT STARTED

AA-sec is deployed and run directly on the client's own infrastructure.

This option is currently in the conceptual phase and not yet under development.

Tailored to your needs.

The chosen deployment method changes where the system runs, but it must not alter the core evidence model, workflows, or audit semantics of AA-sec.

ENGINEERING STATUS

# Current Engineering Status

Our development roadmap reflects key capabilities delivered and those in progress, aligning with our strategic goals for AA-sec.

### READY

- Product lifecycle model
- Release lifecycle / state model
- Built-in scanner / dependency scanning
- SBOM model and governance
- Vulnerability lifecycle workflow
- CRA Article 14 workflow
- Document and dossier generation
- Tenant isolation and encryption model
- Evidence integrity / audit trail

### PARTIAL

- UI surface
- External integrations

### NOT STARTED

- On-prem package

"READY" indicates core capability is functional and usable, not necessarily a fully polished enterprise UI or package.

# CYBER RESILIENCE PLATFORM

SECURE BY EVIDENCE

Built-in scanner.

Evidence graph.

Workflow accountability.

AA-sec turns product-security work into structured, traceable, generated evidence across product, release, vulnerability, CRA workflow, and documentation layers.

**TECHNICAL CAPABILITIES / CONFIDENTIAL DRAFT**