RELIZA

ReARM

Release-Level Supply Chain Evidence Platform

ReARM is a Supply Chain Evidence Platform that Manages and Stores SBOMs, xBOMs and other Security and Compliance Artifacts per Release

https://rearmhq.com

About ReARM

ReARM is an abbreviation for "Reliza's Artifact and Release Management". It is a DevSecOps Digital Asset Management tool to organize product releases with their metadata, including Bills of Materials and other security artifacts (SBOMs / xBOMs).

xBOM Compliance

ReARM allows organizations to maintain up-to-date inventory of digital assets, including SBOMs/xBOMs, in compliance with various regulatory frameworks, including:

- EU CRA, BSI TR-03183, NIS2, DORA
- US EOs 14028, 14144
- Section 524B of the US FD&C Act
- US Army Memorandum on SBOMs
- India RBI and SEBI

Native SDLC Integration

ReARM is designed to work with your Software Development Life Cycle.

ReARM pioneered Product-Component data model describing relationships between Products, Feature Sets, Product Releases, Components, Branches, Component Releases, and their metadata.

This model aligns data representation within ReARM with CI/CD process.

Per Release Metadata

Unlike legacy cybersecurity tools, ReARM stores and processes all metadata per release.

Further, ReARM recognizes that artifacts may belong to the release as a whole, source code entries or deliverables. This allows to establish desired level of granularity when working with security artifacts.

Aggregation Engine

ReARM includes built-in aggregation engine that can automatically merge and profile Bills of Materials, vulnerabilities, weaknesses and policy violation details.

For example, it is possible to produce an aggregated BOM for a Product Release from all its Component Releases in a few clicks.

Capabilities

Inventory

ReARM maintains up-to-date inventory of organization's digital assets, driven by CI/CD tooling

Security Posture

ReARM visualizes security posture for organization's assets with desired level of granularity and builds changelogs

Storage / Retrieval

ReARM allows for storage and retrieval of SBOMs / xBOMs for software and hardware, per release, including signatures and signing details

Aggregation

ReARM allows for seamless creation of aggregated BOMs on Product and Component Release levels

Processing

ReARM supports tight integration with OWASP Dependency-Track, continuously analyzing each SBOM for vulnerabilities and policy violations, with aggregated results available at the release level

Multi-Domain

ReARM enables complex workflows, including combinations of software and hardware components within the same product, making it an invaluable tool in the fields like IoT and medical devices

Why ReARM

- Acts as an audit-ready evidence store that ensures secure and compliant software and hardware supply chains
- Automates end-to-end xBOM workflows, including versioning, changelogs, storage, processing and retrieval
- Includes SBOM augmentation, enrichment, aggregation and filtering capabilities
- Visualizes and manages vulnerability, weakness and policy violation data
- Provides release-level insights
- Integrates natively into CI/CD workflows
- Comes in Pro and Community Editions

The Facts

Core Platform
>5 YEARS
IN PRODUCTION

Storing
>100,000
RELEASES

With
>20
INTEGRATIONS

Comparison with Legacy SBOM Tools

ReARM represents the next generation of release-centric cybersecurity tools. The key differences with previous generation are highlighted in the chart below.

REARM BY RELIZA	LEGACY SBOM TOOLS
Supports variety of SBOM, xBOM, Compliance and Security documents	SBOM-only focused
Artifacts organized by Releases and integrated into Digital Asset Management	Single SBOM for the whole Component
Configurable automated versioning and changelogs	Requires other tooling for versioning and release management
Built-in Approval Workflows supported by evidences	Requires other tooling to capture decisions
Multiple scopes: Organization, Perspective, Product, Component, Release	Usually, only organization-wide scope available