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 Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. – Project: 101190180.

Vulnerability Handling

Digital Innovation Hub Trakia

Co-funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

OSCRAT Open-Source Cyber Resilience Act Tools

About the Lecturer

Lead Auditor for Management Systems, with expertise in information security, artificial intelligence, IT services, quality management, and related domains.

Chairman of the Institute for Artificial Intelligence.

Deputy Manager of the Bulgarian Union of Standardizers.

Active contributor to numerous European and national cybersecurity projects, with a focus on standards, resilience, and digital transformation.

Assistant Professor at UniBIT, teaching:

- Cybersecurity Standards
- Cybersecurity Management
- Cryptography
- Zero Trust Architectures

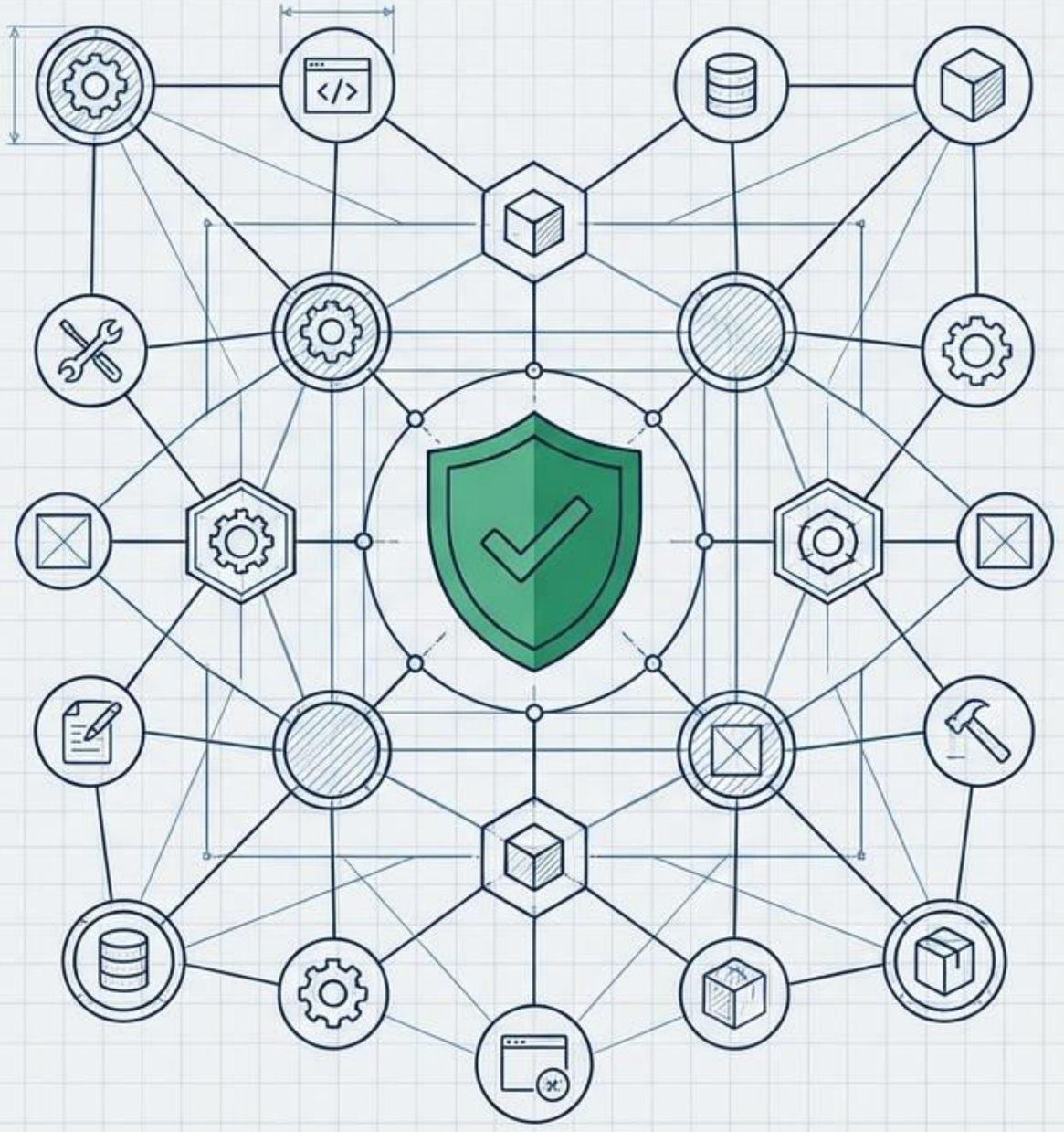
Workshop 3
Vulnerability Handling

- **Session 1: CRA & SBOM in Practice -** Understanding regulatory requirements and how Software Bill of Materials supports transparency and supply chain security.
- **Session 2: OSCRAT Workflow Demonstration -** Live demonstration of the end-to-end vulnerability handling process – scanning, identification, tracking, and reporting.
- **Session 3: Standards & Frameworks -** Overview of key standards and best practices, including ISO, NIST, ENISA, and OWASP, and how they support a structured approach to vulnerability management.

The Cyber Resilience Act & SBOM in Practice

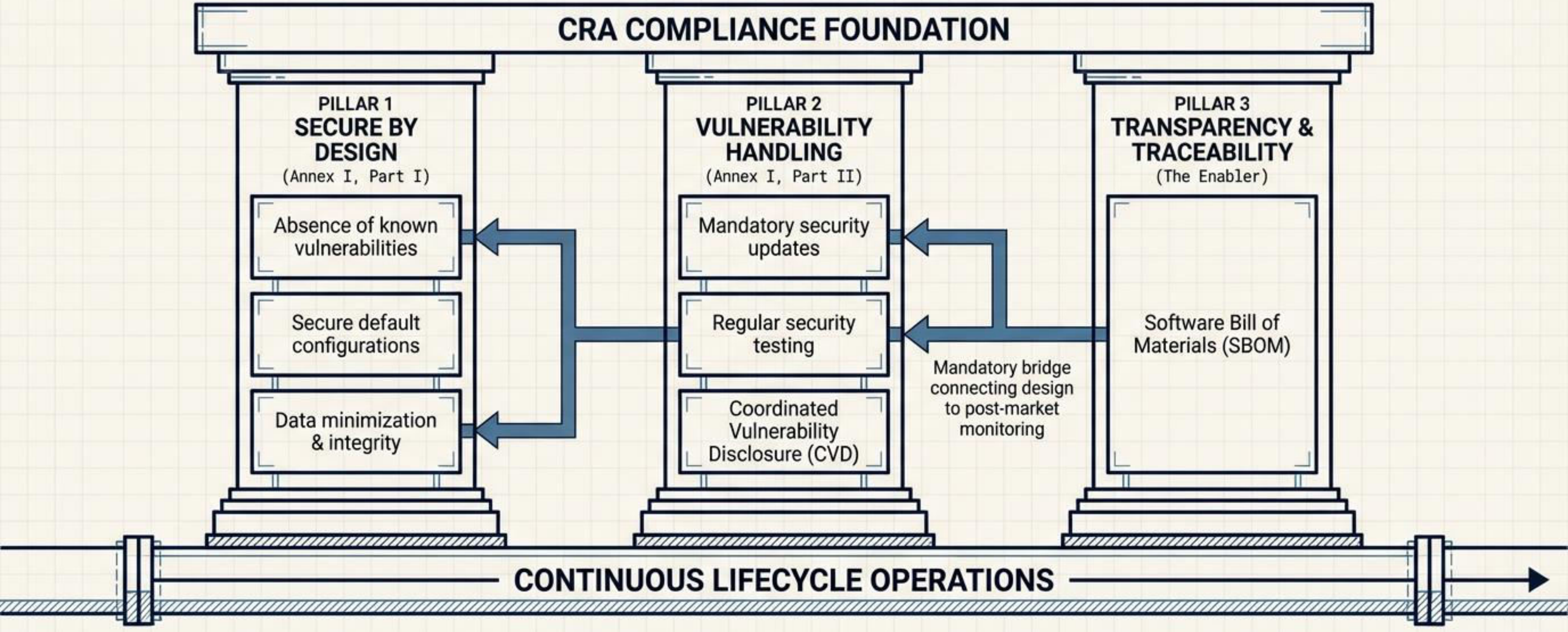
From Regulatory Mandate to DevSecOps Operations.

REGULATION:	EU 2024/2847
SCOPE:	Products with Digital Elements
FRAMEWORK:	Security Lifecycle & Vulnerability Management

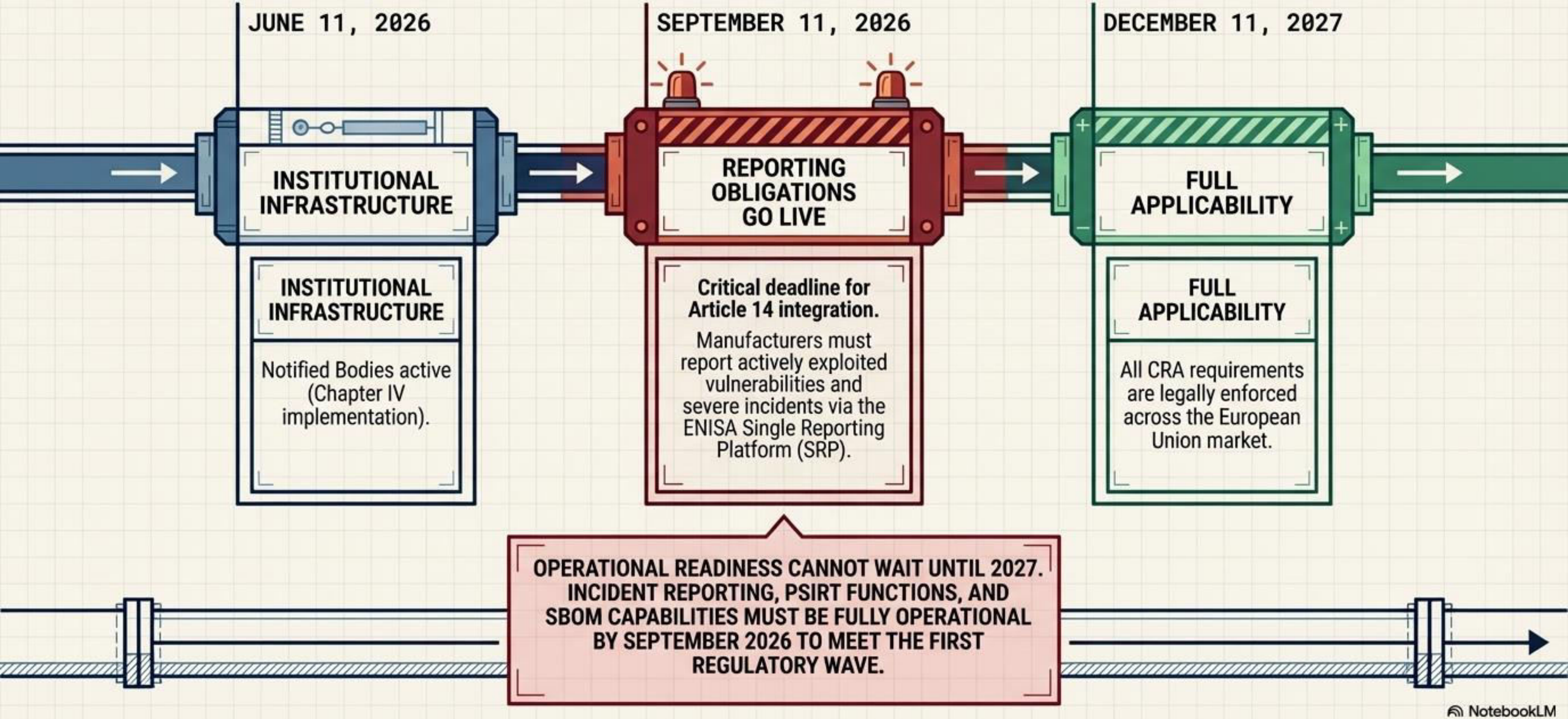


A PERMANENT SHIFT IN MANUFACTURER RESPONSIBILITY

The CRA transitions security from a post-market afterthought to a legally mandated, continuous lifecycle requirement.



THE COUNTDOWN TO COMPLIANCE AND REPORTING OPERATIONS



DEFINING THE SCOPE AND REGULATORY TARGETS

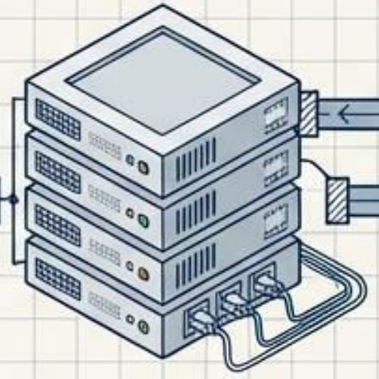
EUROPEAN COMMISSION

MANUFACTURER

Bears the primary regulatory burden. Applies to entities placing products under their own name or trademark, whether for payment, monetization, or free of charge.

IMPORTER

Ensures the manufacturer has complied and drawn up necessary technical documentation before the product enters the EU market.



Product with Digital Elements
(Hardware & Software)

DISTRIBUTOR

Verifies compliance marks and halts distribution if significant cyber risks or non-compliance are identified.

OSS STEWARDS

Open-Source Software entities providing sustained support for commercial activities face tailored, specific obligations under Article 24.

Unpacking the Essential Requirements of Annex I

ANNEX I, PART I

Product Properties (State at Launch)

- Delivered **without known exploitable vulnerabilities**
- Secure by `default` configurations
- Protection of **data integrity** and **confidentiality**
- Minimization of **data footprint**
- Resilience against **denial of service** attacks

ANNEX I, PART II

Vulnerability Handling (Continuous Processes)

- Identify and document components via **machine-readable** SBOM
- Address vulnerabilities without delay
- Provide security updates **separate from feature** updates
- Execute regular **security testing** and reviews
- Enforce a Coordinated Vulnerability Disclosure (CVD) policy

Crucial Insight: The CRA does not stop at "Secure-by-Design". It demands a sustainable, provable process for vulnerability management throughout the product's active lifespan.

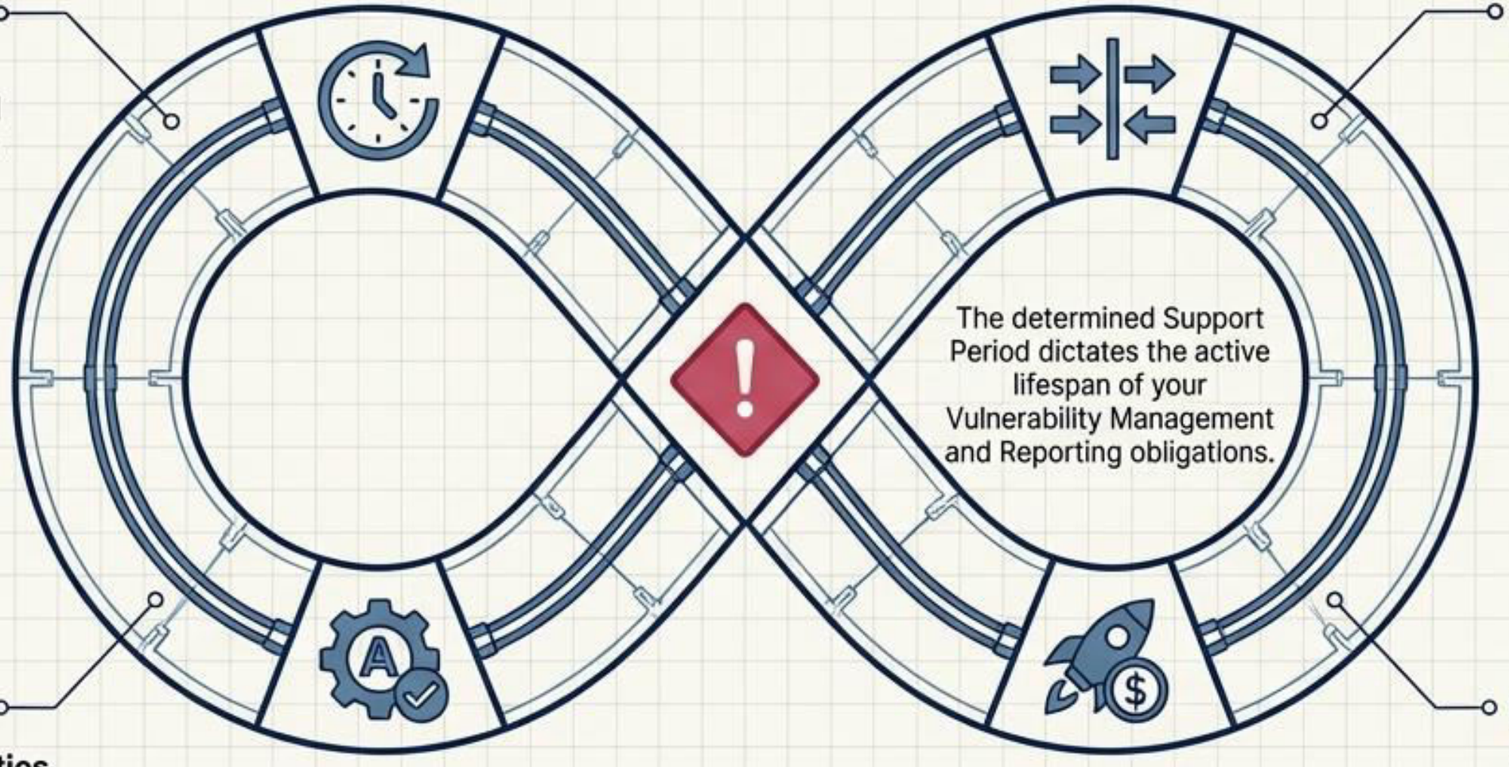
The Support Period & Security Update Mandate

Support Duration

Manufacturers must determine a support period of at least 5 years (unless the expected product lifetime is shorter).

Separation of Concerns

Security updates must be distributed **separately** from functional or feature upgrades to ensure **rapid deployment**.



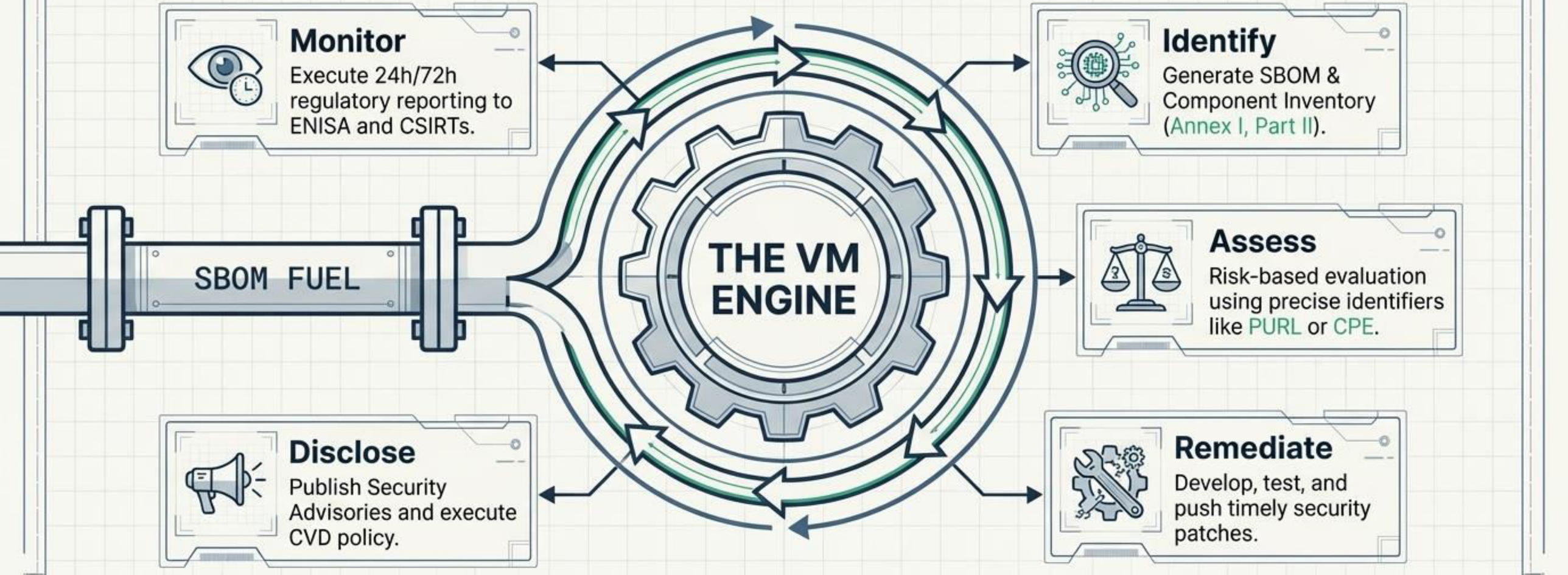
Automation

Automatic update capabilities are required by default, featuring a clear and transparent user **opt-out mechanism**.

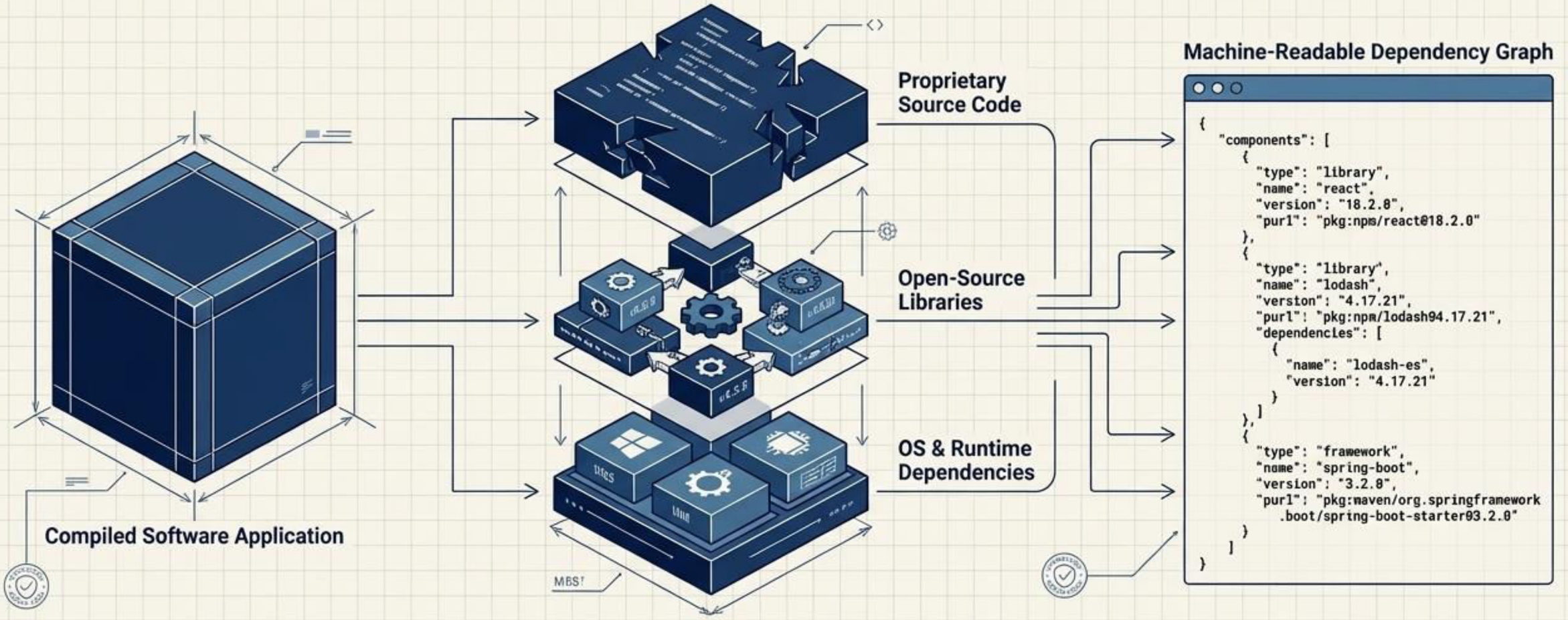
Cost & Velocity

Security patches must be delivered **without delay**, **free of charge** to the user throughout the support period.

Translating Legal Mandates into the Vulnerability Management Workflow



The Software Bill of Materials (SBOM) as the Compliance Bridge



The Core Premise: You cannot remediate, patch, or report a vulnerability within a strict 24-hour legal window if you lack an automated, machine-readable inventory. SBOM is the mandatory fuel for CRA compliance.

SBOM Standards Face-Off: CycloneDX vs. SPDX

Evaluating utility strictly through the lens of CRA compliance and Vulnerability Management.

Dimension	CycloneDX (v1.7)	SPDX (v3.0.1)
Primary Focus	Supply chain security, precise dependencies, and VEX.	Package licensing, deep component relationships, and legal compliance.
Vulnerability / VEX Support	Native, first-class objects for vulnerability disclosure and VEX routing.	Relies heavily on external identifiers and profiles for VM workflows.
Serialization	JSON, XML, Protobuf.	Defined semantic data model supporting multiple format serializations.
CRA & DevSecOps Fitness	Highly practical for automated DevSecOps pipelines and VM integration.	Excellent for deep compliance auditing and complex legal tracing.

Note: The CRA does not legally mandate one specific standard, but emerging technical profiles (e.g., BSI TR-03183-2) require validation against either format.

Constructing the Target CRA SBOM Profile

Machine-Readable SBOM JSON Snippet

```
{
  "bomFormat": "CycloneDX",
  "specVersion": "1.5",
  "serialNumber": "urn:uuid:3e671687-395b-41f5-a30f-a58921a69b79",
  "version": 1,
  "metadata": {
    "timestamp": "2023-10-27T12:00:00Z",
    "tools": [
      {
        "vendor": "ACME Solutions",
        "name": "SBOM Generator",
        "version": "2.0.1"
      }
    ],
    "component": {
      "type": "application",
      "name": "Critical Infra Core",
      "version": "1.0.0",
      "purl": "pkg:generic/critical-infra-core@1.0.0"
    }
  },
  "components": [
    {
      "type": "library",
      "name": "SecureLib",
      "version": "3.2.1",
      "purl": "pkg:npm/securelib@3.2.1",
      "cpe": "cpe:2.3:a:securelib:securelib:3.2.1:*:*:*:*:*:*:*",
      "licenses": [...]
    },
  ],
  "dependencies": [
    {
      "ref": "pkg:generic/critical-infra-core@1.0.0",
      "dependsOn": [
        "pkg:npm/securelib@3.2.1"
      ], }
    { "ref": "pkg:npm/securelib@3.2.1",
      "dependsOn": [
        "pkg:npm/transitive-dep@1.1.0"
  ] } }
}
```

Format Specification

JSON or XML serialization only. Must be strictly machine-readable.

Dependency Depth

Recursive dependency resolution. Must capture top-level dependencies and traverse transitively to enable accurate chaining.

Required Minimum Metadata

Must explicitly include Creator, Timestamp, Component Name, Version, and stable Identifiers (PURL/CPE).

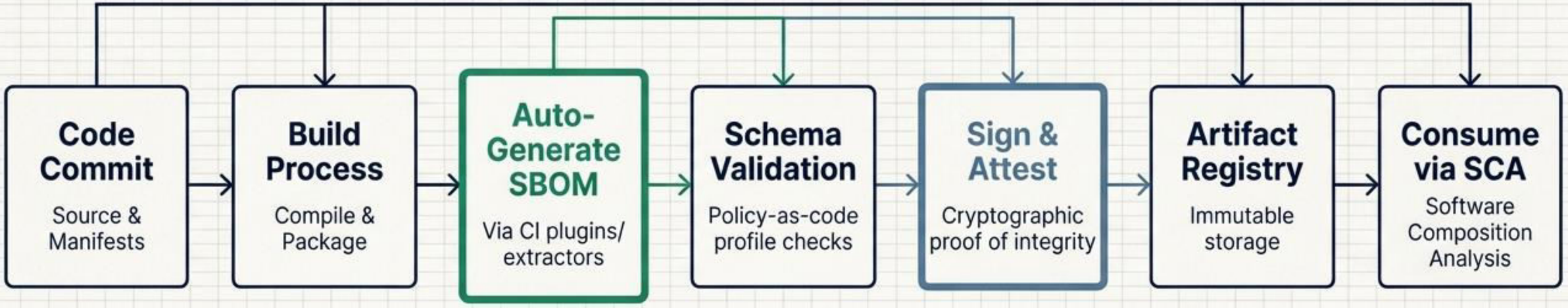
Statelessness Principle

The SBOM must remain static to the specific build version. Dynamic vulnerability data (VEX) should be maintained as a separate, associated.

VERIFIED COMPLIANCE

BSI TR-03183-2 PROFILE SATISFIED

The Continuous CI/CD Automation Pipeline



WARNING: Manual SBOM generation is dead. It is fundamentally incompatible with modern release cadences and strict CRA reporting timelines.

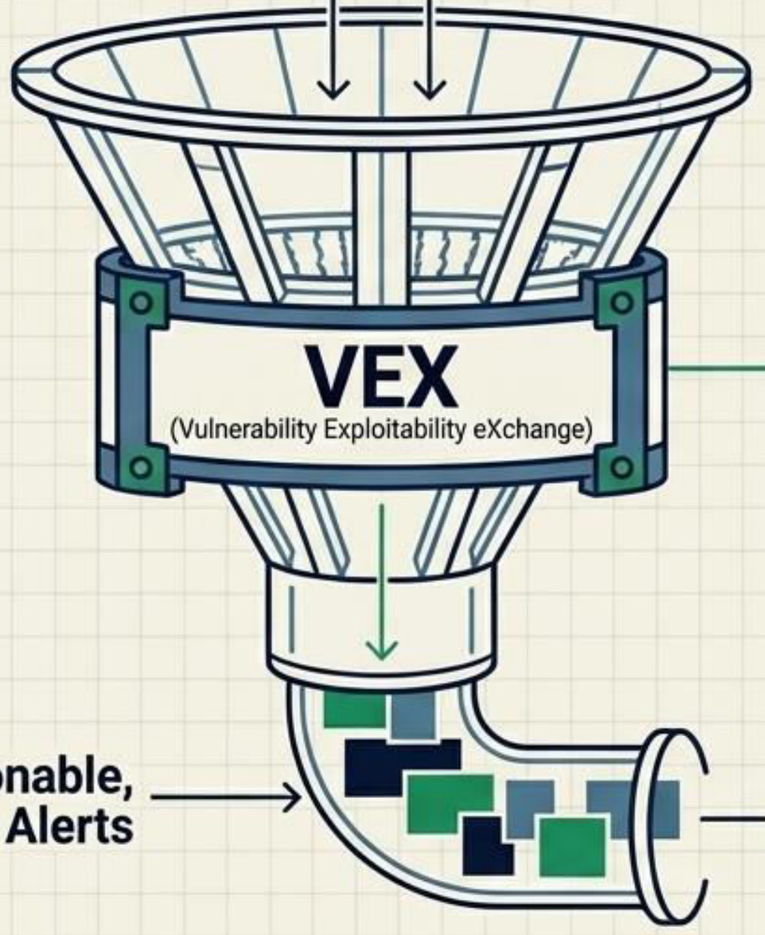
Supercharging Vulnerability Management with VEX

Signed SBOM

Static structural component list

CVE Databases & Advisories

Dynamic threat intelligence



VEX adds crucial context. It provides **machine-readable assertions** that a vulnerable component is present, but the specific vulnerable code path is **unreachable** or **mitigated**.

Actionable, Prioritized Alerts

Impact:

- Drastically reduces “False Positive” noise, saves critical engineering time, and aligns with CRA risk-based assessment mandates.

The CRA Incident Reporting Decision Tree (Article 14)

TRIGGER: Actively exploited vulnerability OR severe incident detected.

24-Hour Early Warning

Submitted to ENISA Single Reporting Platform (SRP) and CSIRT.

72-Hour Full Notification

Provides general information, exploitation nature, and mitigation details.

Remediation Action

Security patch deployed or mitigation applied.

Final Report: 14 Days

Due 14 days after a vulnerability remediation becomes available.

Final Report: 1month

Due 1 month after an incident notification.

USER COMMUNICATION TRACK

Simultaneously inform affected users about the incident/vulnerability and provide clear mitigation instructions.

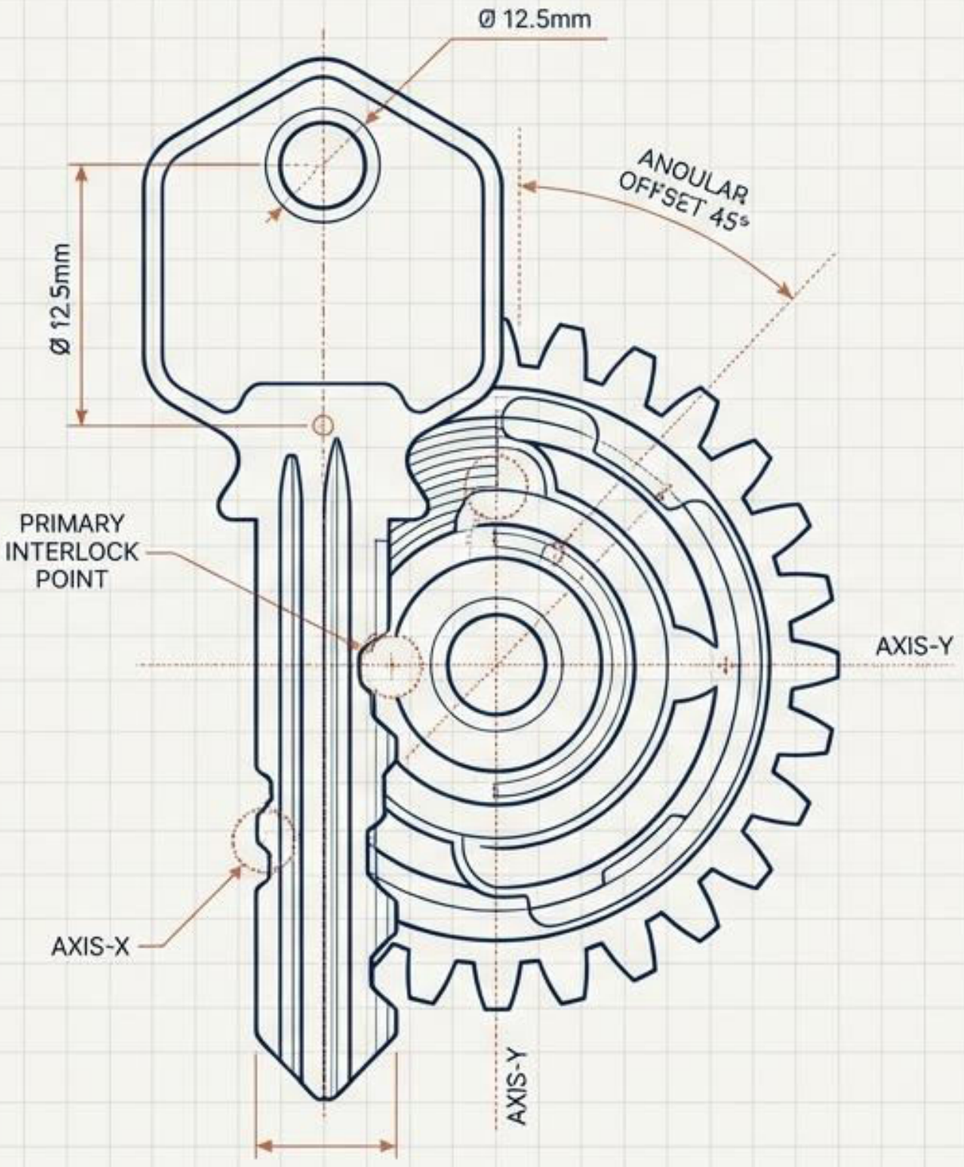
The CRA Readiness Matrix

Strategic Action	Primary Owner	Target Deadline
Define Support Period & Map Ecosystem Roles	Product Management / Legal	Q2 2026
Establish Coordinated Vulnerability Disclosure (CVD) Policy & Public security.txt	PSIRT / Communications	Q3 2026
Implement CI/CD SBOM Automation & Cryptographic Signing	DevSecOps / Engineering	September 2026
Integrate ENISA SRP Reporting Runbooks & 24h Triage Workflows	PSIRT / Compliance	September 2026

Beyond Compliance: The New Standard for Software Trust

The **Cyber Resilience Act** is not a paperwork exercise. It is a fundamental architectural shift toward continuous, transparent, and automated supply chain security.

Start building your automation pipeline today. The critical reporting window opens in **September 2026**.



Vulnerability Management: Standards & Frameworks

A **Strategic Blueprint** to the ISO, NIST, ENISA, and OWASP Ecosystems

Navigating the complete lifecycle from secure design to coordinated disclosure and enterprise patching.

The Six Pillars of Vulnerability Management

ENISA Security by Design

Pre-release. Building security in from day one.

NIST SP 800-40

End-User Defense. Enterprise Patch Management.

OWASP Dependency-Check

Development. Securing the software supply chain.

No single standard covers everything. True resilience requires integrating these interlocking frameworks across the software lifecycle.

ENISA CVD

Macro Policy. Coordinated Vulnerability Disclosure.

ISO/IEC 29147

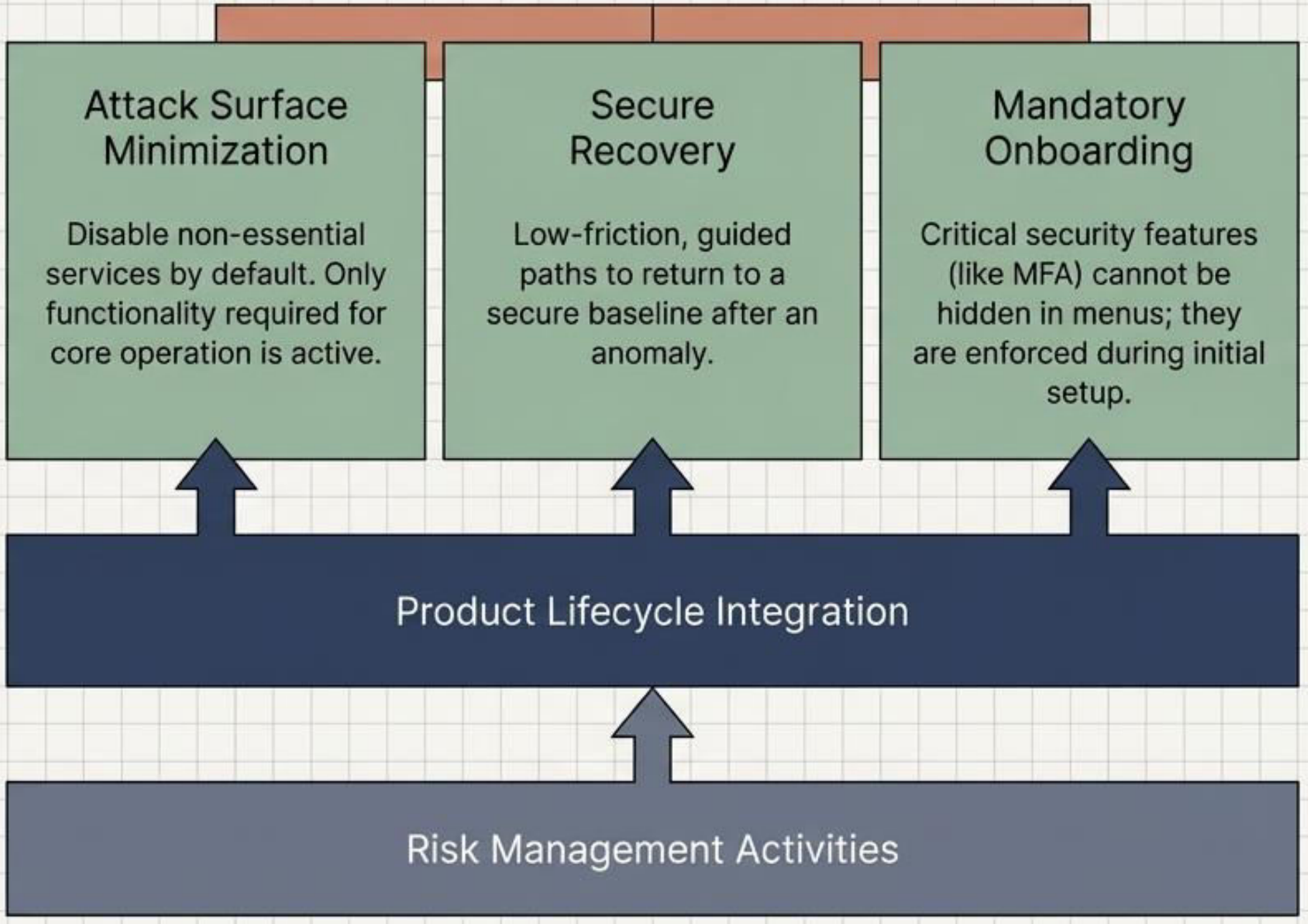
External Interface. Vulnerability Disclosure.

ISO/IEC 30111

Internal Engine. Vulnerability Handling.

ENISA Security by Design (SbD)

Based on the upcoming comprehensive guide (targeted March 2026), moving SbD from theoretical concept to engineering reality. Eradicate vulnerabilities before they are written.



OWASP Dependency-Check: Software Composition Analysis

The Problem

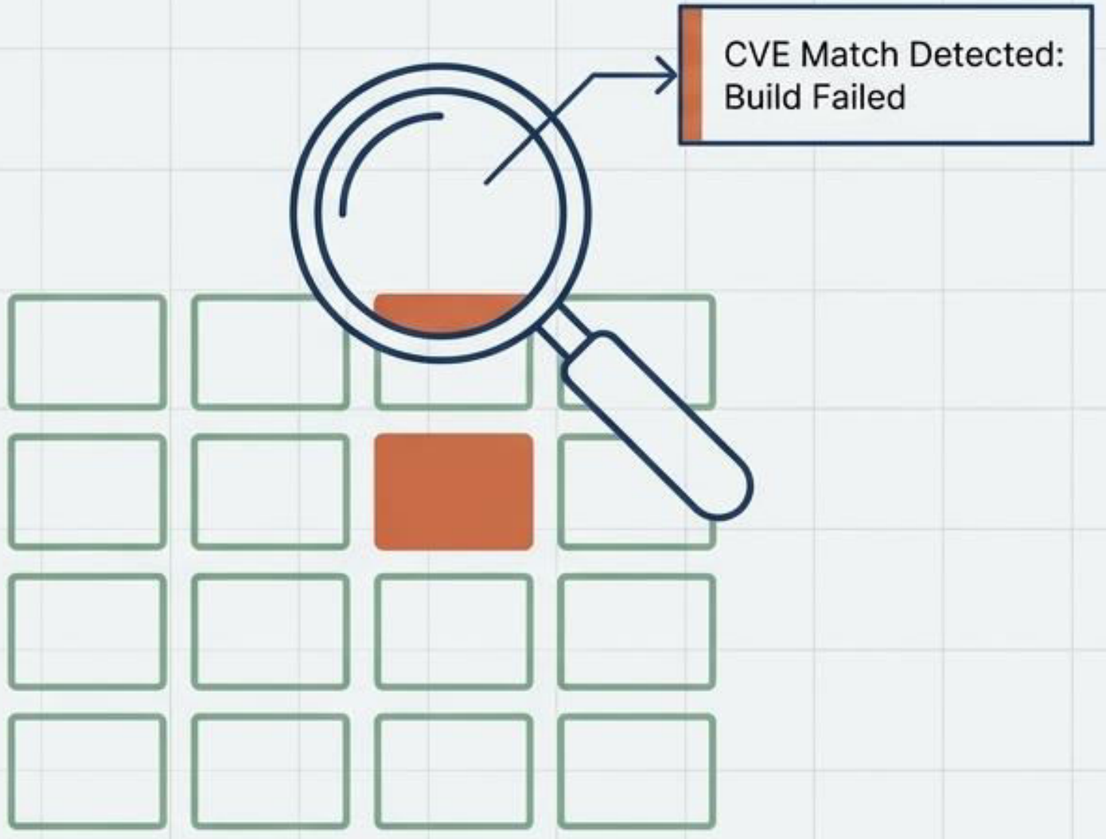
Modern applications are assembled, not written. Patching dependencies requires code changes and full regression testing.

The Solution

An automated SCA utility that identifies project dependencies and checks if there are publicly disclosed vulnerabilities (`CVEs`) mapped via the National Vulnerability Database (NVD).

Implementation

Integrates directly into the CI/CD pipeline (`Maven`, `Gradle`, `Jenkins`) to act as a quality gate, automatically failing builds if known critical vulnerabilities are detected.



software build

ISO/IEC 29147: The External Interface

Establishing safe, standardized interactions between vendors and external vulnerability finders.

Disclosure Policy (VDP)

Publish clear guidelines outlining safe harbor provisions, scope, and reporting expectations.

Secure Receipt

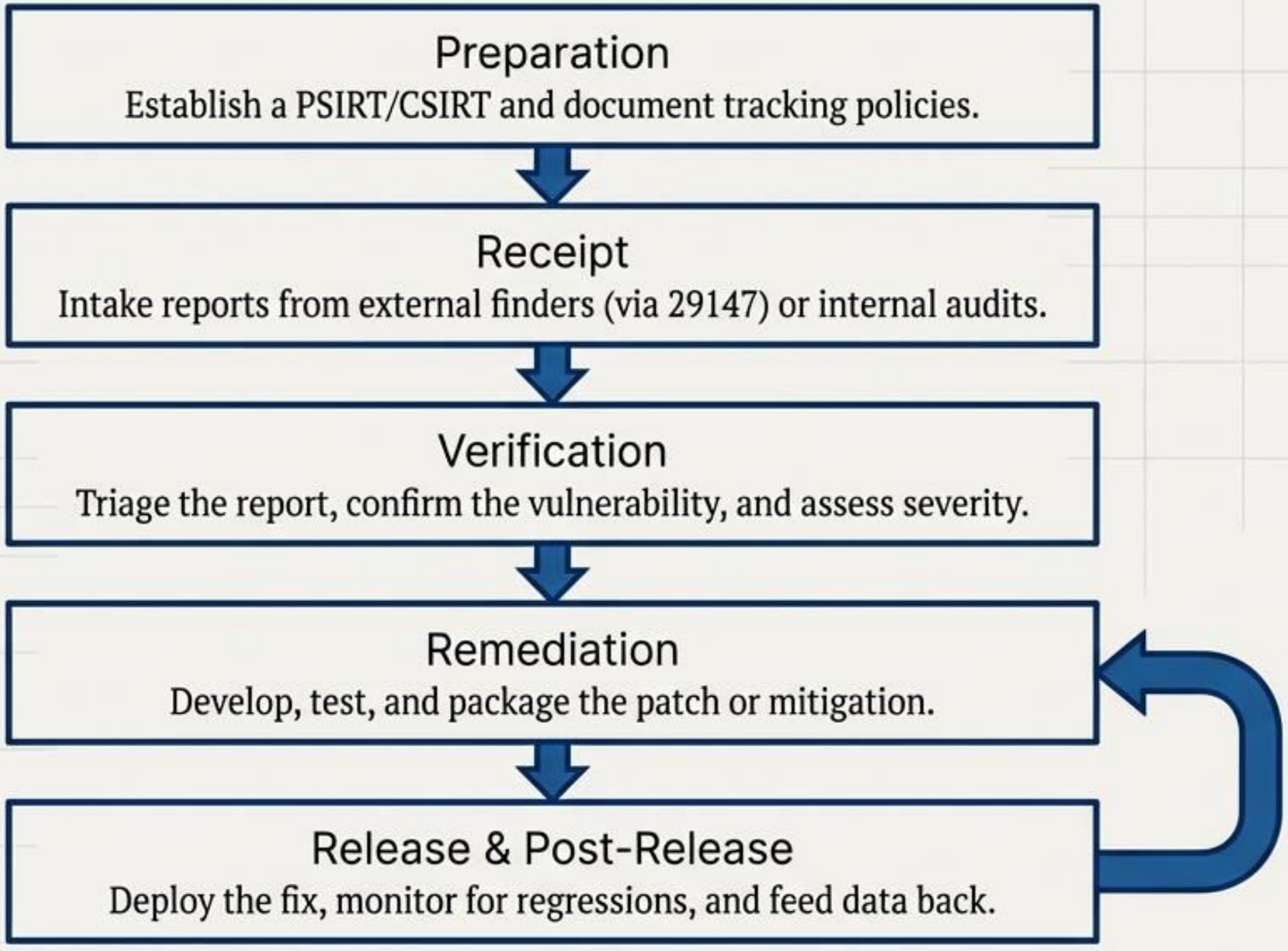
Provide confidential reporting mechanisms (e.g., HTTPS web forms, TLS) so sensitive exploit data is not intercepted.

Standardized Advisories

Publish consistent remediation information with clear severity ratings (like CVSS) to allow users to make informed risk decisions.

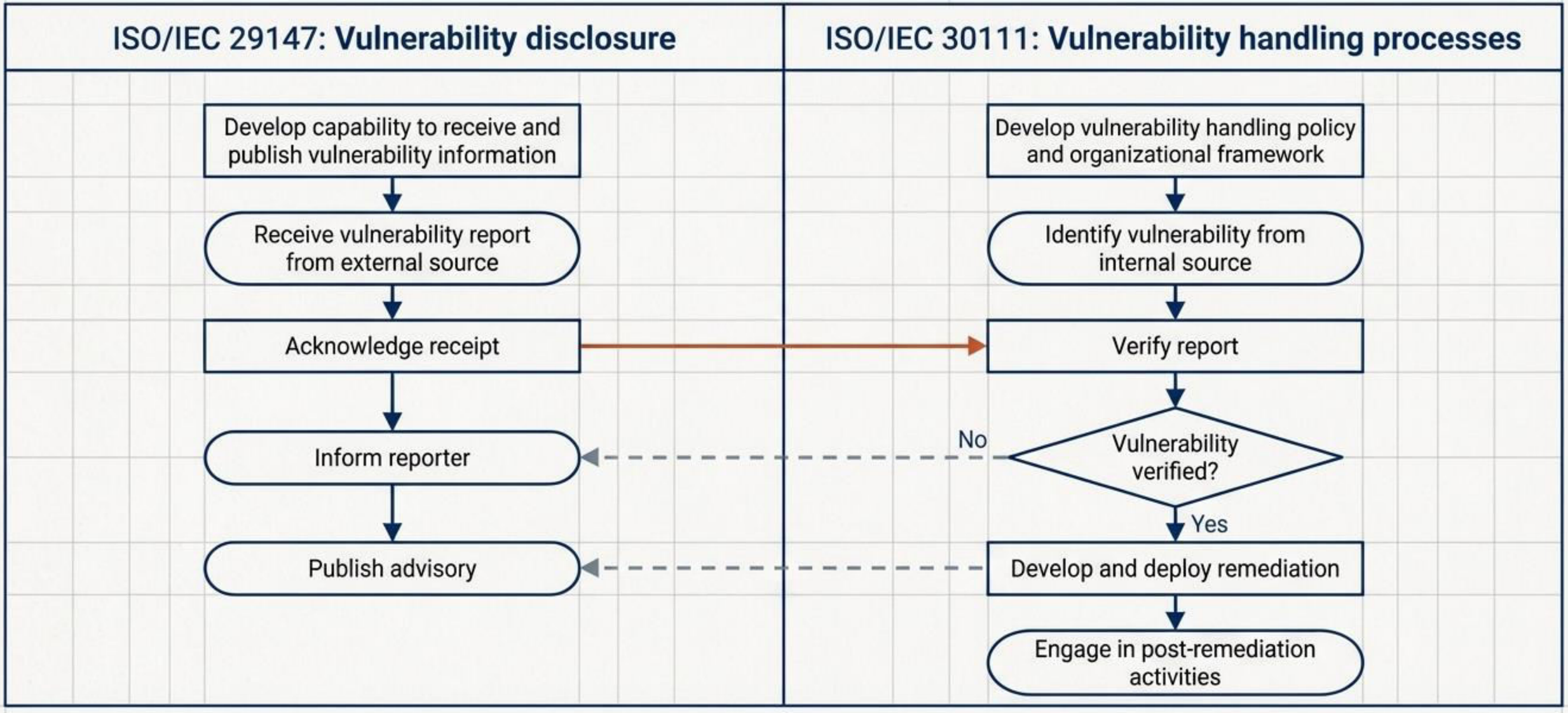
ISO/IEC 30111: The Internal Engine

The internal processes vendors use to investigate, triage, and resolve vulnerabilities.



The Disclosure-Handling Symbiosis

ISO 29147 acts as the front door interfacing with the public. ISO 30111 operates as the kitchen processing the fix. They are mutually dependent.



ENISA CVD: The Macro Policy Level

Harmonizing Coordinated Vulnerability Disclosure across national borders to protect ethical hackers and systemic infrastructure.

Legal Safe Harbor

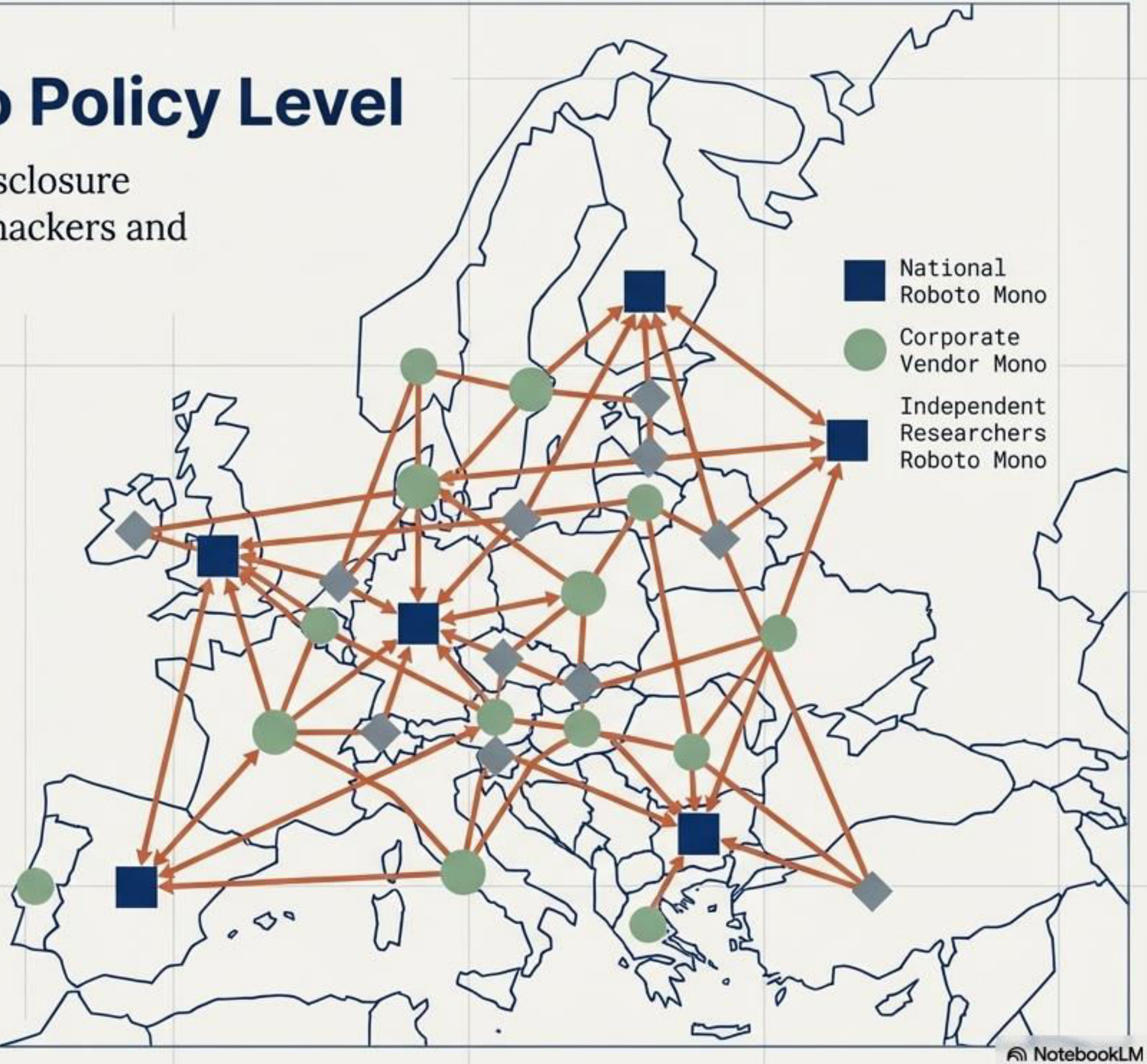
Defining the role of ethical hackers in national law to prevent prosecution for good-faith security research.

The Coordinator Role

Utilizing National CSIRTs/CERTs as neutral mediators, especially when multiple vendors are affected or unresponsive.

Ecosystem Incentives

Encouraging bug bounties and active participation from the global security research community.



NIST SP 800-40: Enterprise Patch Management

The Mindset Shift: Patching is not an IT burden; it is preventive maintenance and a fundamental cost of doing business.

Simplify & Automate	Maintenance Groups	Accept the Friction
It is impossible to manually risk-assess every CVE. Use automation to scale deployments swiftly.	Segment enterprise assets based on risk and apply pre-defined response scenarios (Routine, Emergency, Unpatchable).	Occasional operational disruption from a patch is a necessary, acceptable trade-off to prevent catastrophic network compromise.

Synthesis 1: The Lifecycle Intersection

Creation Phase

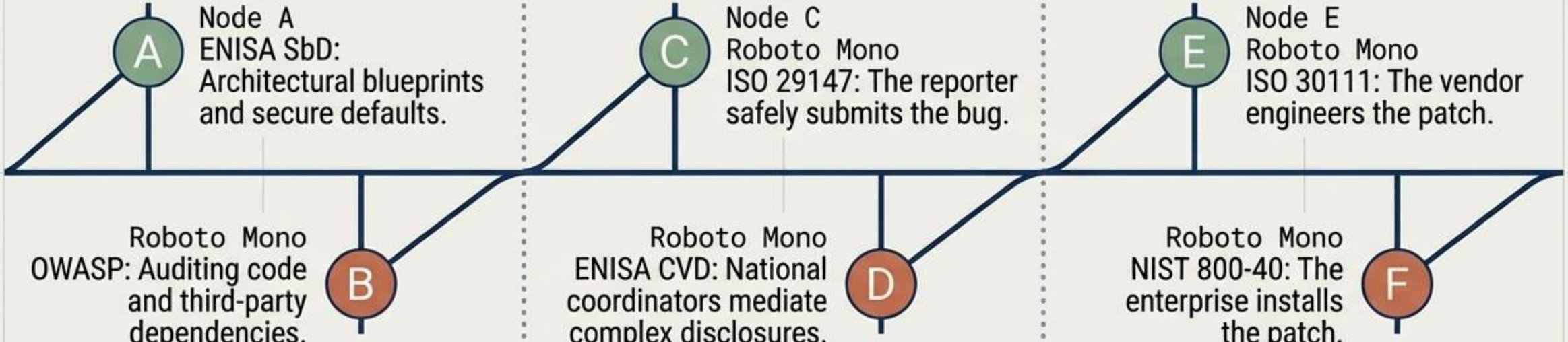
Prevent vulnerabilities from shipping.

Discovery Phase

Safe, structured communication of flaws.

Operation Phase

Swift risk reduction and execution.



Creation Phase

Prevent vulnerabilities from shipping.

Discovery Phase

Safe, structured communication of flaws.

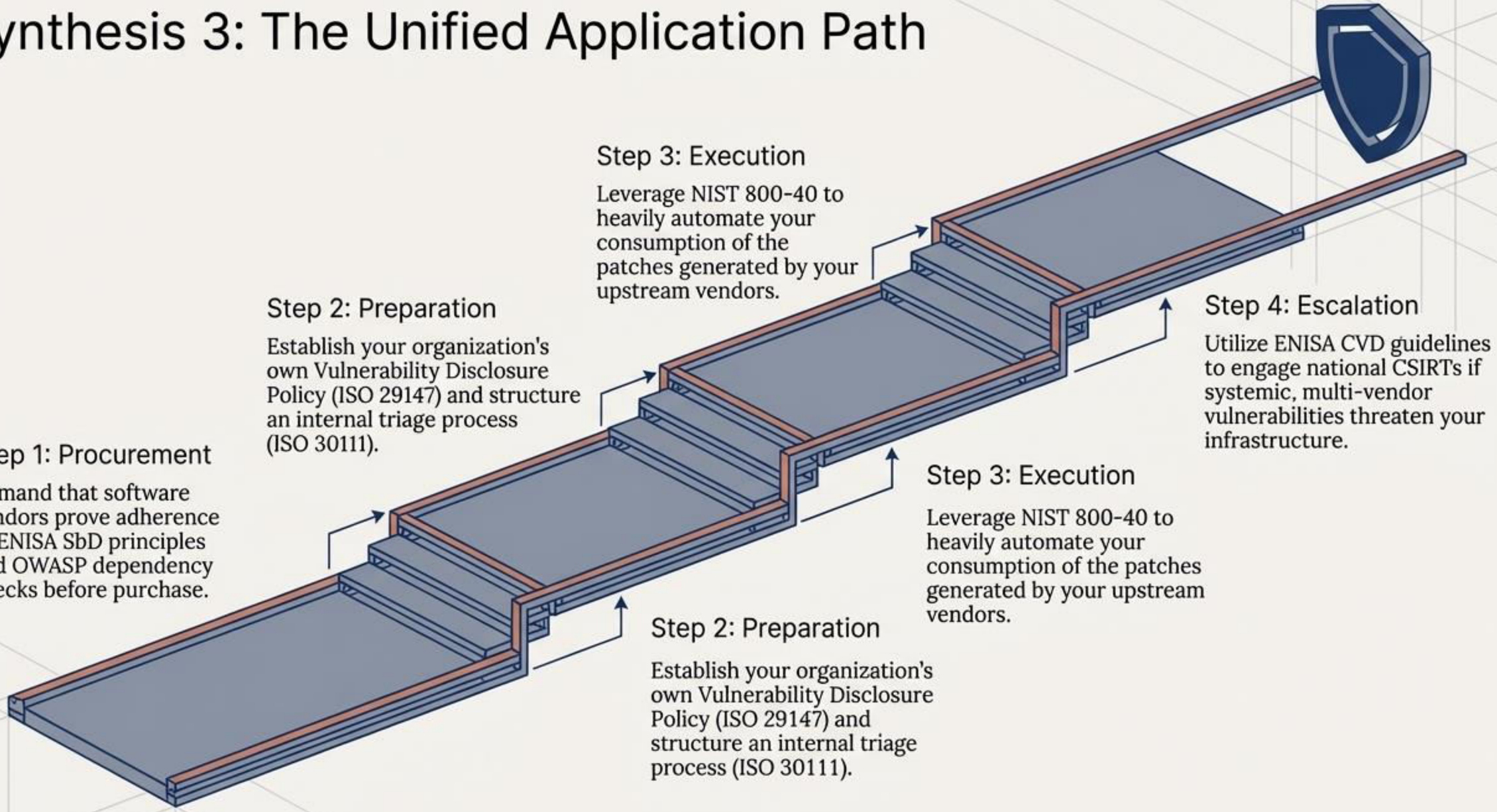
Operation Phase

Swift risk reduction and execution.

Synthesis 2: The Stakeholder Matrix

Framework	Primary Actor	Key Output	Core Objective
OWASP Dependency-Check	Developers	Clean Code / SBOM	Supply Chain Security
ISO 30111 & ENISA SbD	Software Vendors	Secure Products & Patches	Product Integrity
ISO 29147 & ENISA CVD	Coordinators & Researchers	Advisories & VDP Policies	Transparent Disclosure
NIST SP 800-40	Enterprise IT / Security	Updated Assets	Operational Defense

Synthesis 3: The Unified Application Path



Step 1: Procurement

Demand that software vendors prove adherence to ENISA SbD principles and OWASP dependency checks before purchase.

Step 2: Preparation

Establish your organization's own Vulnerability Disclosure Policy (ISO 29147) and structure an internal triage process (ISO 30111).

Step 3: Execution

Leverage NIST 800-40 to heavily automate your consumption of the patches generated by your upstream vendors.

Step 4: Escalation

Utilize ENISA CVD guidelines to engage national CSIRTs if systemic, multi-vendor vulnerabilities threaten your infrastructure.

Step 2: Preparation

Establish your organization's own Vulnerability Disclosure Policy (ISO 29147) and structure an internal triage process (ISO 30111).

Step 3: Execution

Leverage NIST 800-40 to heavily automate your consumption of the patches generated by your upstream vendors.

Conclusion: A Holistic Security Posture

01 Shift Left & Right

Security is not a single phase. It requires proactive action at code inception (OWASP, SbD) and continuous defensive operation (NIST, ISO).

02 Communication is Security

Standardized disclosure (CVD, 29147) prevents operational chaos, protects ethical researchers, and delivers fixes to users faster.

03 Automation & Policy

Without automation, enterprise patching fails. Without policy, disclosure fails. Architect both to survive the modern threat landscape.

Next workshop
Risk Management

- Identify and assess risks using likelihood and impact
- Apply appropriate risk treatment strategies: accept, reduce, avoid, or transfer
- Maintain a structured risk register linked to tasks and supporting evidence
- Ensure full traceability and auditability of risk-related decisions

Date: 27 April 2026

Platform: Zoom

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 Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. – Project: 101190180.

Thank you!

Miroslav Mitev, PhD
+359 896 198 875
phdmitev@gmail.com

Digital Innovation Hub Trakia

Co-funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

OSCRAT Open-Source Cyber Resilience Act Tools