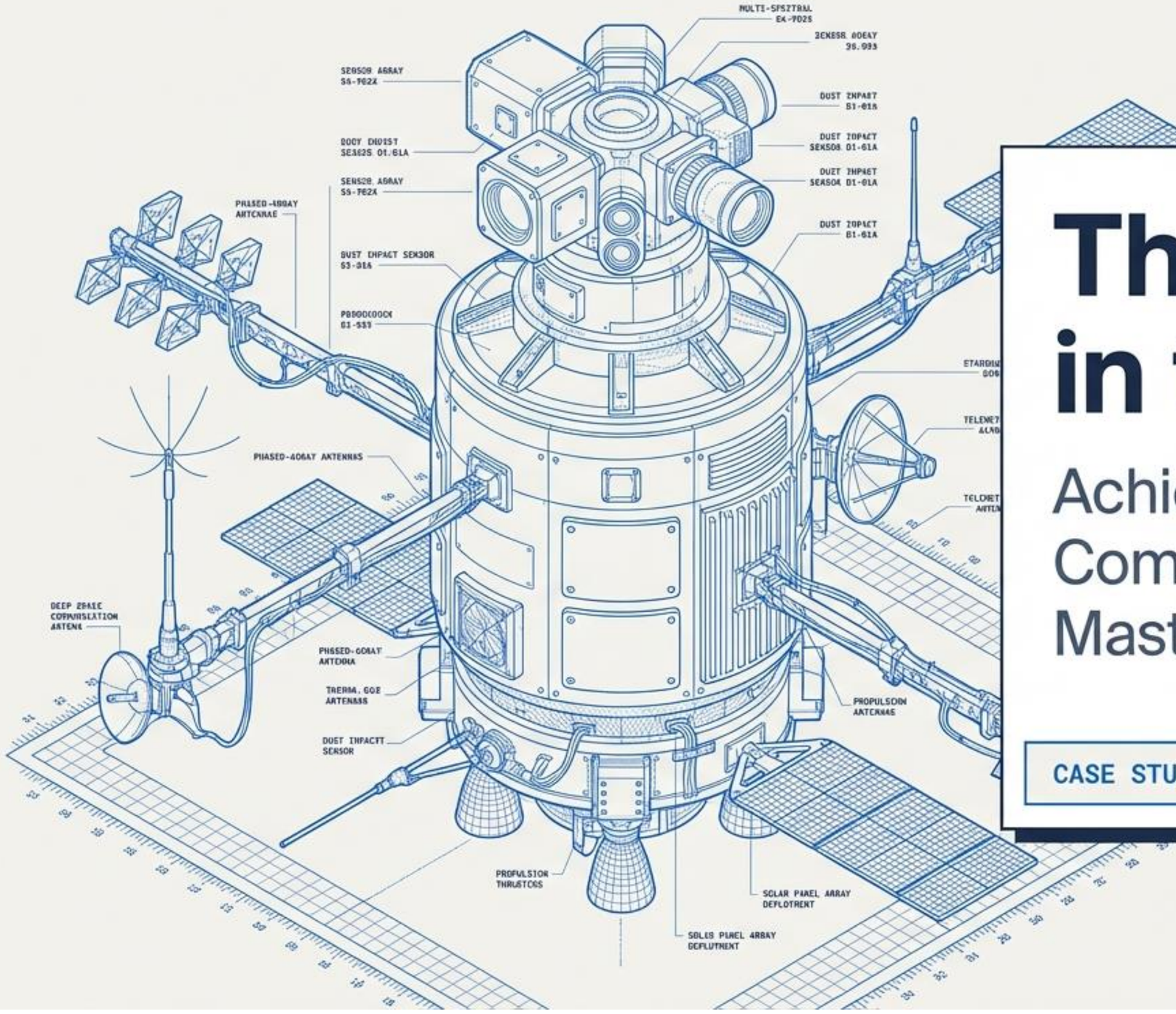


The Signal in the Noise

Achieving CRA Compliance and Mastering Risk with VEX

CASE STUDY: STARDUST METEOR DUST ANALYZER

The CRA Mandate

> **“No known exploitable vulnerabilities.”**

Market Gatekeeper

Must be achieved and proven before initial market placement.

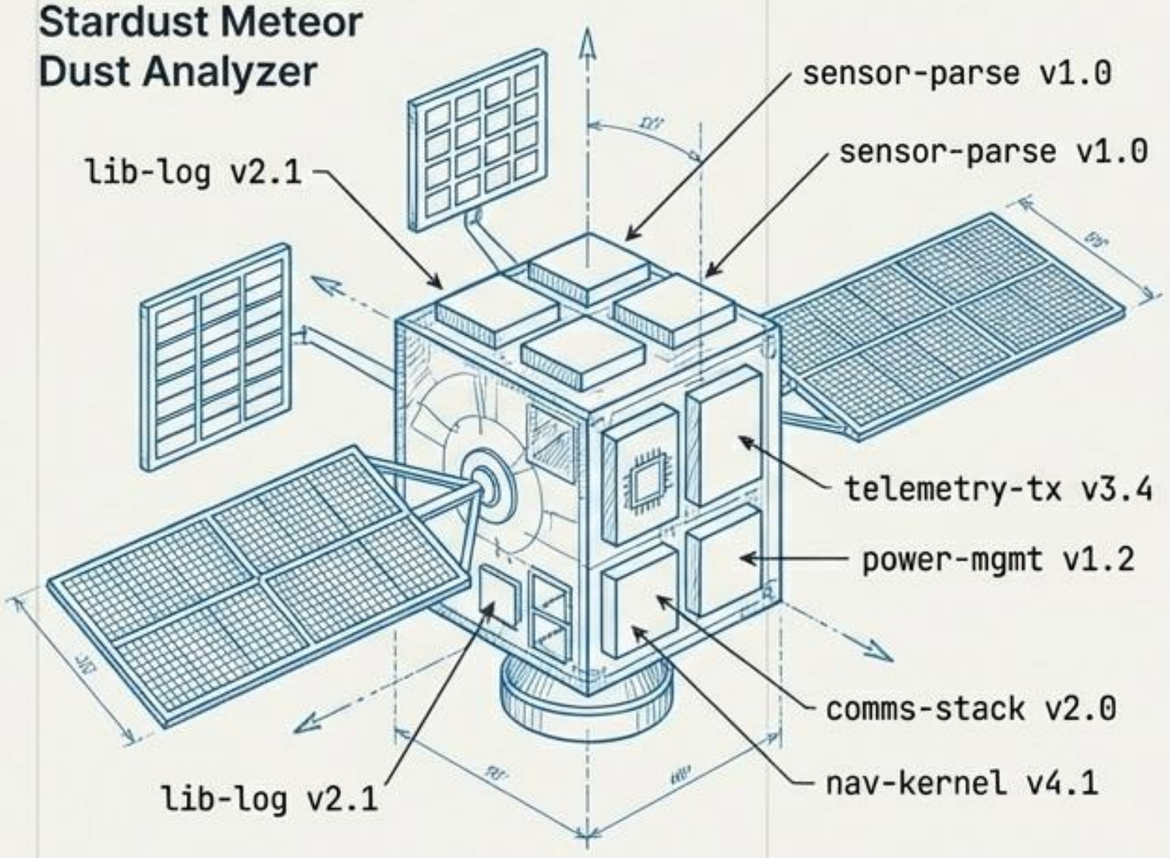
Continuous Lifecycle

Requires continuous vulnerability handling throughout the product support period.

Strict Reporting

Mandatory ENISA reporting: **24h** for actively exploited, **72h** for severe vulnerabilities.

The Reality of the SBOM Scan




```
[ALERT] 500 Vulnerabilities Detected in Stardust OS

CVE-2025-1011 - CRITICAL - sensor-parse
CVE-2025-2042 - HIGH - lib-log
CVE-2025-3099 - CRITICAL - telemetry-tx
CVE-2025-4105 - MEDIUM - power-mgmt
CVE-2025-5218 - CRITICAL - comms-stack
CVE-2025-6320 - HIGH - nav-kernel
...
```

Dilemma: If the CRA demands zero known exploitable vulnerabilities, how does the Stardust launch on time with 500 red flags?

The Compliance Pipeline

01. SBOM Generation
Raw Input & Unfiltered CVEs

02. VEX Context Engine
Applicability & Engineering Triage

03. Final Risk Matrix
Structured Output & CRA Evidence

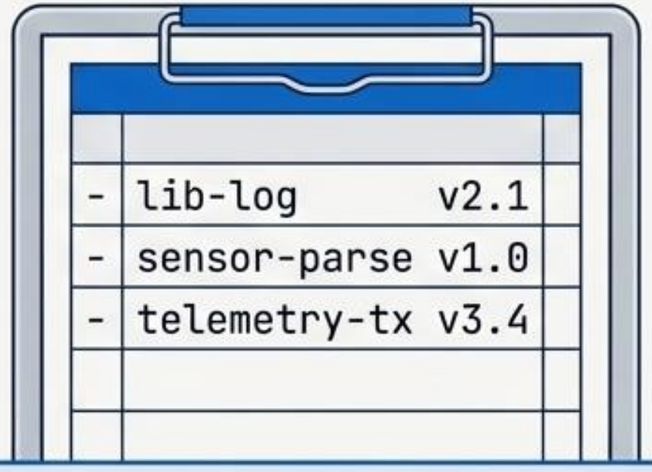
We cannot fix 500 theoretical vulnerabilities.
We must filter for the reality of our environment.

The Inventory vs. The Impact

SBOM

(Software Bill of Materials)

What is in the box?



Identifies components and known CVEs, but entirely ignores how the software is configured or executed.

VEX

(Vulnerability Exploitability eXchange)

Is it dangerous to me?

Assesses vulnerabilities against the specific architecture, compensating controls, and usage of the product.

The Vulnerability Funnel

INPUT: 500 Raw CVEs from SBOM

STATUS: NOT_AFFECTED
Catches: 450 CVEs

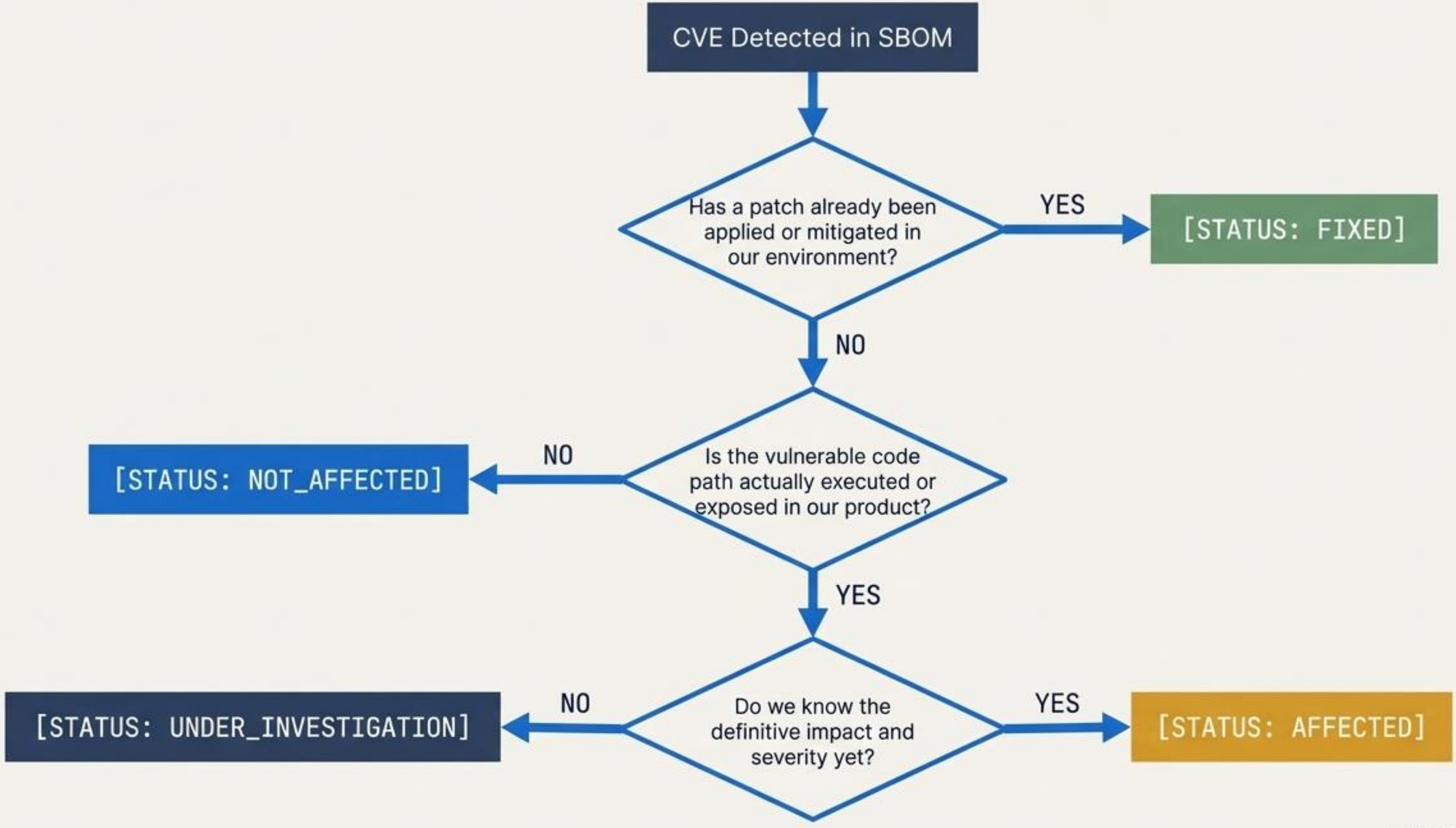
STATUS: FIXED
Catches: 40 CVEs

STATUS: UNDER_INVESTIGATION
Catches: 8 CVEs

OUTPUT: AFFECTED
Result: 2 actionable CVEs

VEX mathematically reduces compliance panic by systematically eliminating false positives.

The Context Triage Tree



The VEX Diagnostic Matrix

VEX Status	CRA Impact	Required Action	Stardust Example
[NOT_AFFECTED]	Compliant	Document Justification	CVE in lib-log, but the logging module is permanently disabled in Stardust firmware.
[FIXED]	Compliant	Verify Patch	Sensor array vulnerability heavily patched in Stardust OTA update v1.2.
[UNDER_INVESTIGATION]	Pending	Triage Rapidly	Analyzing if the new sensor-parse CVE affects our specific data pipeline.
[AFFECTED]	Blocks Compliance	Patch & Report (24h/72h)	Known memory leak in the live telemetry transmitter. Requires immediate fix.

Machine-Readable Standards

VEX must scale. You cannot track this in spreadsheets. Ensure automation by utilizing standardized, machine-readable specification formats.

CycloneDX VEX

- Native VEX support integrated directly.
- Best option if you are already generating CycloneDX SBOMs in your CI/CD pipeline.
- Unified file approach.

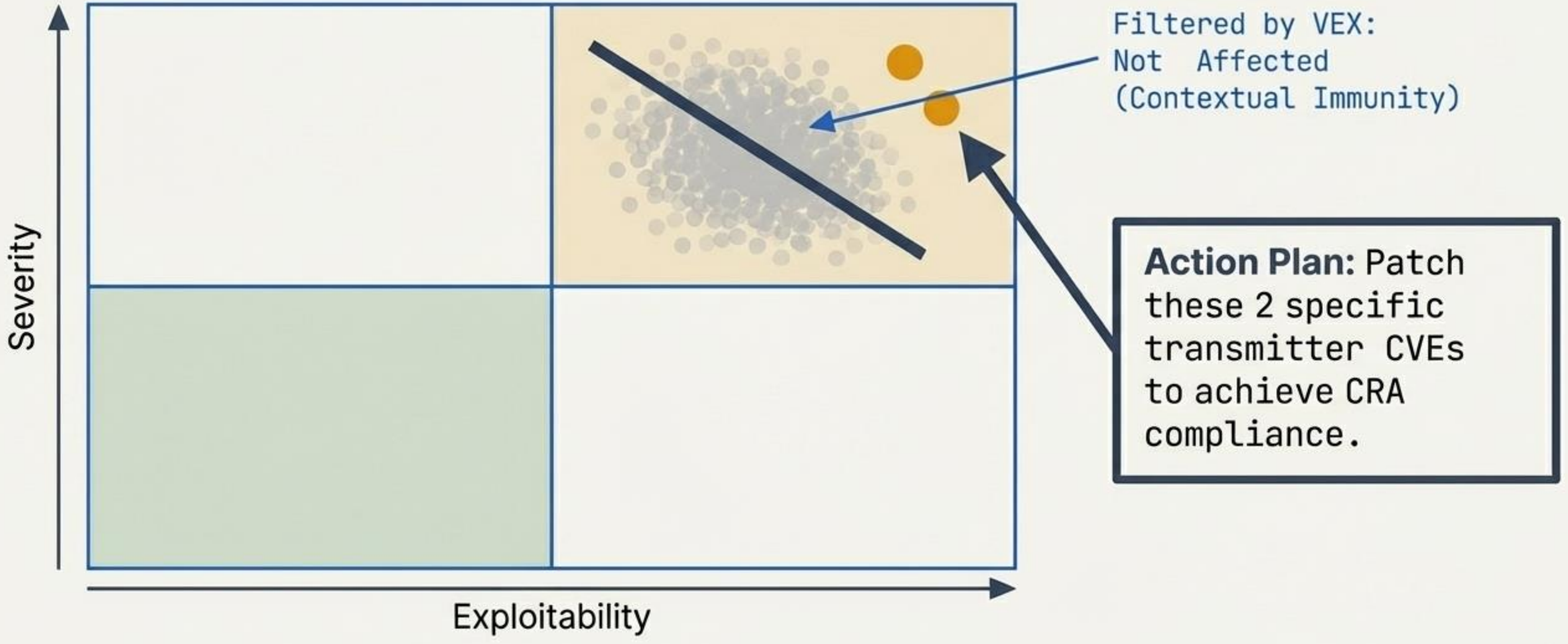
CSAF

- Common Security Advisory Framework.
- Robust, standalone VEX document format.
- Ideal for complex, multi-vendor advisories and deep vulnerability metadata.

OpenVEX

- Simpler, highly focused VEX format.
- Built specifically for rapid pipeline integration and minimal overhead.
- Easy to generate programmatically.

The Exploitability Matrix



VEX isolates the true risk. We do not halt production for 500 theoretical issues; we engineer fixes for 2.

Continuous Compliance at Scale

The Reality of Decay

Vulnerability status is highly dynamic; new CVEs are published daily.

Manual technical analysis for every new scan blocks engineering velocity.

ENISA reporting mandates strict, unforgiving timelines (24h/72h).

Automated Evidence

Automate Rescanning: Implement trigger-based VEX generation on new CVEs or firmware version bumps.

Justification Templates: Build pre-approved, machine-readable patterns for common Stardust architecture defenses.

CRA Evidence Platform: Manage VEX alongside SBOMs, dynamically mapping status to the technical file for regulators.

VEX transforms compliance from an impossible math problem into a manageable engineering workflow. It is the only way to find the signal in the SBOM noise.

// Note: Despite the scary name, VEX is not short for Vecna from *Stranger Things*. It is here to save your product launch, not drag it into the Upside Down.