OBSERVATORY INTRODUCES

SOFTWARE SUPPLY CHAIN VULNERABILITY DETECTION

93%

YEAR-ON-YEAR INCREASE IN SOFTWARE SUPPLY CHAIN ATTACKS

CYBLE

$138B

PROJECTED GLOBAL LOSSES FROM SOFTWARE SUPPLY CHAIN ATTACKS

CYBERSECURITY VENTURES

ZERO

EASM PLATFORMS PROVIDING SOFTWARE SUPPLY CHAIN VULNERABILITY DETECTION

Discover the software packages running on your internet-facing assets, without needing to access the source code, and map them to known vulnerabilities.

THE HIDDEN ATTACK SURFACE

What is the software supply chain?

Modern applications are assembled from dozens of components; building from scratch is impossible at scale. A single app may depend on hundreds of open-source packages, each with its own dependencies. These external components, which are not your proprietary code, are a target for supply chain attacks.

Why don't organisations know what they're running?

Transitive dependencies stack invisibly: you import Library A, A imports B, B imports C. At an enterprise scale, apps run thousands of indirect dependencies that are not manually catalogued. When a package is compromised, many organisations do not know if they are running it.

How did we get here?

The IT world evolved towards abstraction and reuse. Each step made the software faster to build, but added more layers of external dependency. AI has accelerated this further: AI-generated code often pulls in packages the developer didn't consciously choose.

THE GAP OBSERVATORY CLOSES

Software Composition Analysis (SCA) tools operate inside the development pipeline. **None of them see what you've actually deployed to the internet** - Observatory bridges that gap.

OBSERVATORY'S DEEPER VULNERABILITY DETECTION

DEEP FIELD

Observatory already discovers internet-facing assets on your attack surface and maps known CVEs and other vulnerabilities against them. Now, our AI models provide unparalleled runtime vulnerability detection for parts of your software ecosystem not covered by DevOps tools—this is especially important for teams not on a unified developer infrastructure, such as contractors, 3rd-party suppliers, subsidiaries, and new groups following M&A activity.

Package-Level Detection

Proprietary scanning identifies the specific third-party packages running on your internet-facing assets, down to the version level.

Two Dimensions of Supply Chain Visibility in One Platform

View your vendors' software supply chain to gain deeper visibility into supply chain risk. Observatory combines traditional supply chain monitoring with Deep Field Analytics. When a package is compromised, you can assess exposure across your own estate and important third parties.

Continuous Monitoring

As new CVEs are disclosed or new attacks emerge, continuous scanning means you find out before attackers do.

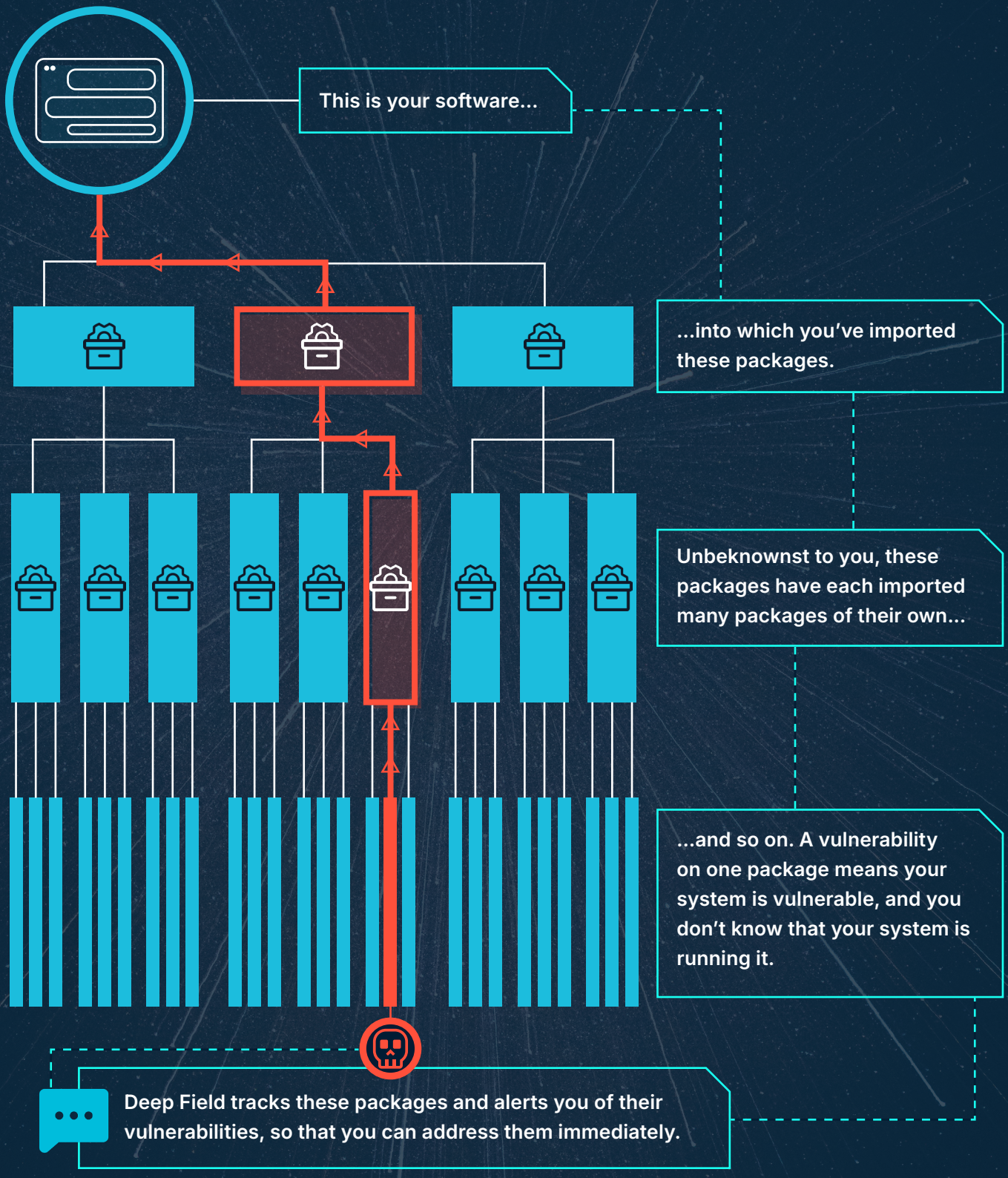
Automatic CVE Mapping

Every detected package is mapped to its known CVEs and enriched with CVSS, EPSS, and Known Exploited Vulnerability (KEV) data so they can be assessed for exploitability and criticality.

Compliance Requirements

The EU Cyber Resilience Act (enforcing December 2027), US Executive Order 14028, NIS2, and DORA all now require organisations to know what software is running across their own estate and their critical vendors.

YOUR SOFTWARE'S SUPPLY CHAIN



GET BETTER ANSWERS FASTER

Faster answer to “Are we running the compromised package?” when a zero-day breaks.

Evidence of deployed (not just declared) components for audit and regulatory reporting.

Prioritised vulnerability backlog based on real-world exploitability (EPSS, KEV, and in-house testing), not just raw CVSS.

Visibility into critical vendors’ exposed software stack, without access to their source or pipelines.

A central point of truth for your software supply chain.

LEARN MORE AND JOIN THE WAITING LIST:

ACDS

ADVANCED CYBER DEFENCE SYSTEMS

ACDSGLOBAL.COM