VicOne

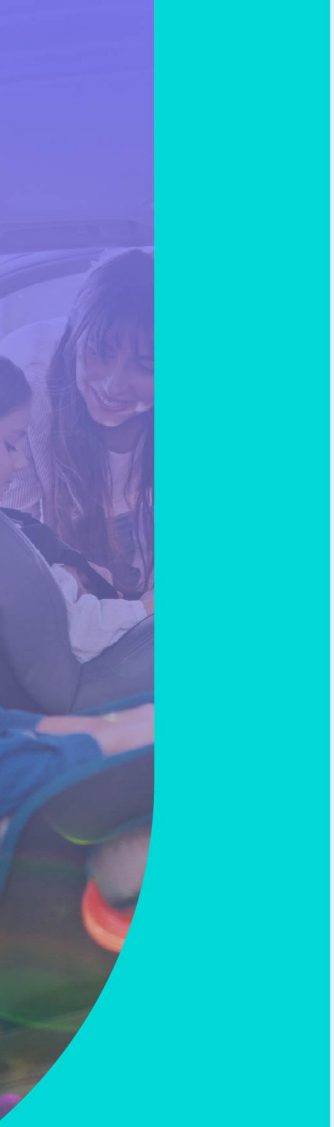
USE CASE

From Manual to One-Click

Identify Software's Country of Origin With xZETA

Overview of US Rule on Connected Vehicle Technologies From ‘Countries of Concern’

Regulatory framework	US Code of Federal Regulations Title 15 Part 791 – Securing the Information and Communications Technology and Services Supply Chain (Effective January 2021) └Subpart D: ICTS Supply Chain: Connected Vehicles (Effective March 2025)
Covered vehicles	Passenger vehicles weighing less than 10,001 pounds (approximately 4,500 kg) • Commercial vehicles are expected to be included in future regulatory phases. Construction equipment, agricultural machinery, and rail systems are currently excluded.
Covered systems	Software and hardware that enable the following systems: • VCS: vehicle connectivity system • ADS: automated driving system
Regulated model years	• Software: applies to model year 2027~ • Hardware: applies to model year 2030~ • For vehicle types without a designated model year, the rule applies starting in 2029. • Exemption: Software that was designed, developed, manufactured, or supplied before March 17, 2026, is excluded from the regulation.
Approval process	Annual declaration of compliance: • Due diligence • Documentation and recordkeeping of supporting evidence
Penalties	• Subject to criminal enforcement • Willful violations might result in up to US$1 million in fines or 20 years in prison, or both.



Affected Parts

- Application
- Middleware
- System software
- Open-source software components that have been modified for proprietary purposes and are not redistributed or shared
- Exclusion: open-source software
- Exclusion: firmware

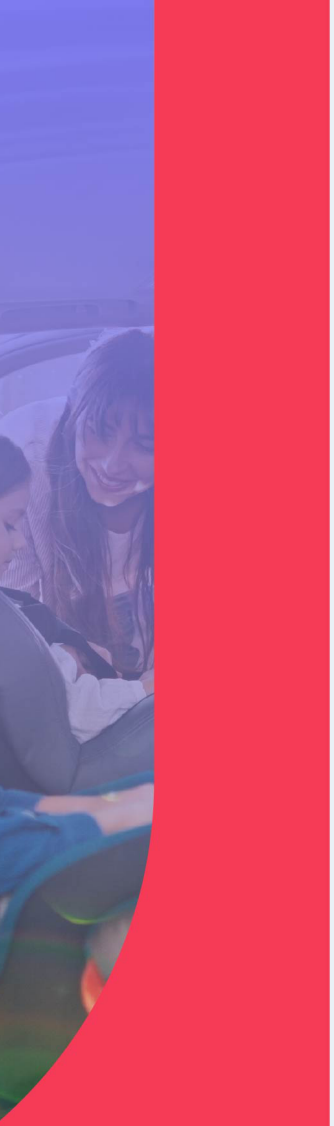
VCS

- Installed in/on connected vehicles
- Systems that enable RF transmission or processing over 450 MHz

Exclusions: automotive sensors, ultrawideband communications, unidirectional RF bands, and components that supply or manage power for the VCS

ADS

Systems that directly enable SAE Level 3 or higher autonomous driving capabilities



SBOM-Related Requirements

Under the US connected vehicle technologies rule, there is a requirement to record partial elements of the software bill of materials (SBOM) either through an SBOM itself or other methods.

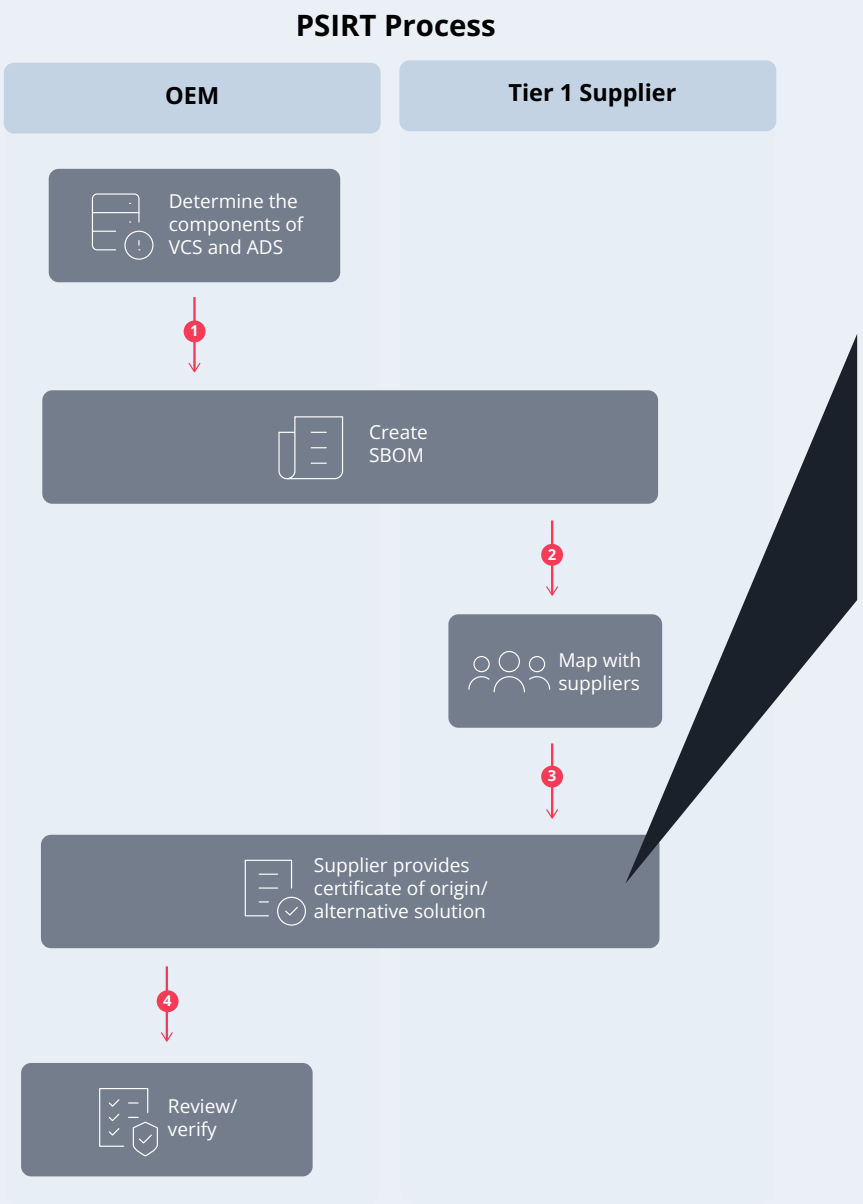
Regulation	EU Cyber Resilience Act	US Executive Order 14028 (Improving the Nation's Cybersecurity)	US Connected Vehicle Regulations (15-CFR Part 791 Subpart D)
Purpose	Protecting users and consumers from a cybersecurity perspective	Strengthening the security of US government infrastructure and critical infrastructure	Regulating the import of products from "countries of concern" to protect national security
Definition of SBOM	Covering at least the highest-level dependencies of the product, in a commonly used machine-readable format	An official record detailing the various components used in software construction and their relationships within the supply chain	
Requirements	**SBOM creation requirements:** • Highest-level dependencies: the main component and its first-level dependencies • Common formats: SPDX, CycloneDX, etc.	**Practical requirements for SBOM creation:** • *Component records* • Author name • Supplier name • Timestamp • Component name • Component version • Unique identifier	**Practical requirements for SBOM creation:** • *Component records* • Author name • Supplier name • Timestamp • Component name *Recorded via SBOM or other methods

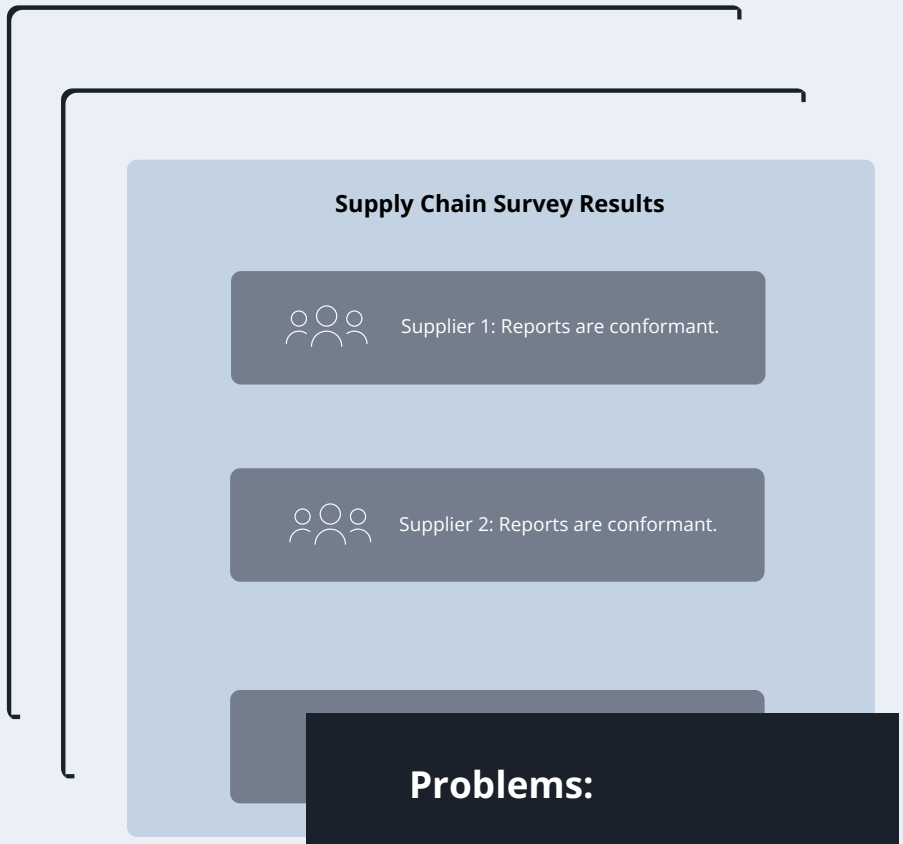
Key Requirements for Compliance Declaration Regarding Covered Software

The primary responsibility lies with the OEM. Suppliers are required to cooperate with due diligence efforts, maintain and document necessary records, and, in some cases, submit information directly to the US Department of Commerce.

	OEM	Supplier
Submission of compliance declaration to the US Department of Commerce	✓	
Proof that the design, development, manufacturing, and supply were not conducted by individuals affiliated with countries of concern	✓	Cooperation
Due diligence	✓	Cooperation
Recordkeeping and retention of covered software for 10 years, with submission upon request by the US Department of Commerce	✓	✓
Proof of having taken all necessary measures to obtain and evaluate required records from suppliers	✓	Cooperation

The Current Common Practice

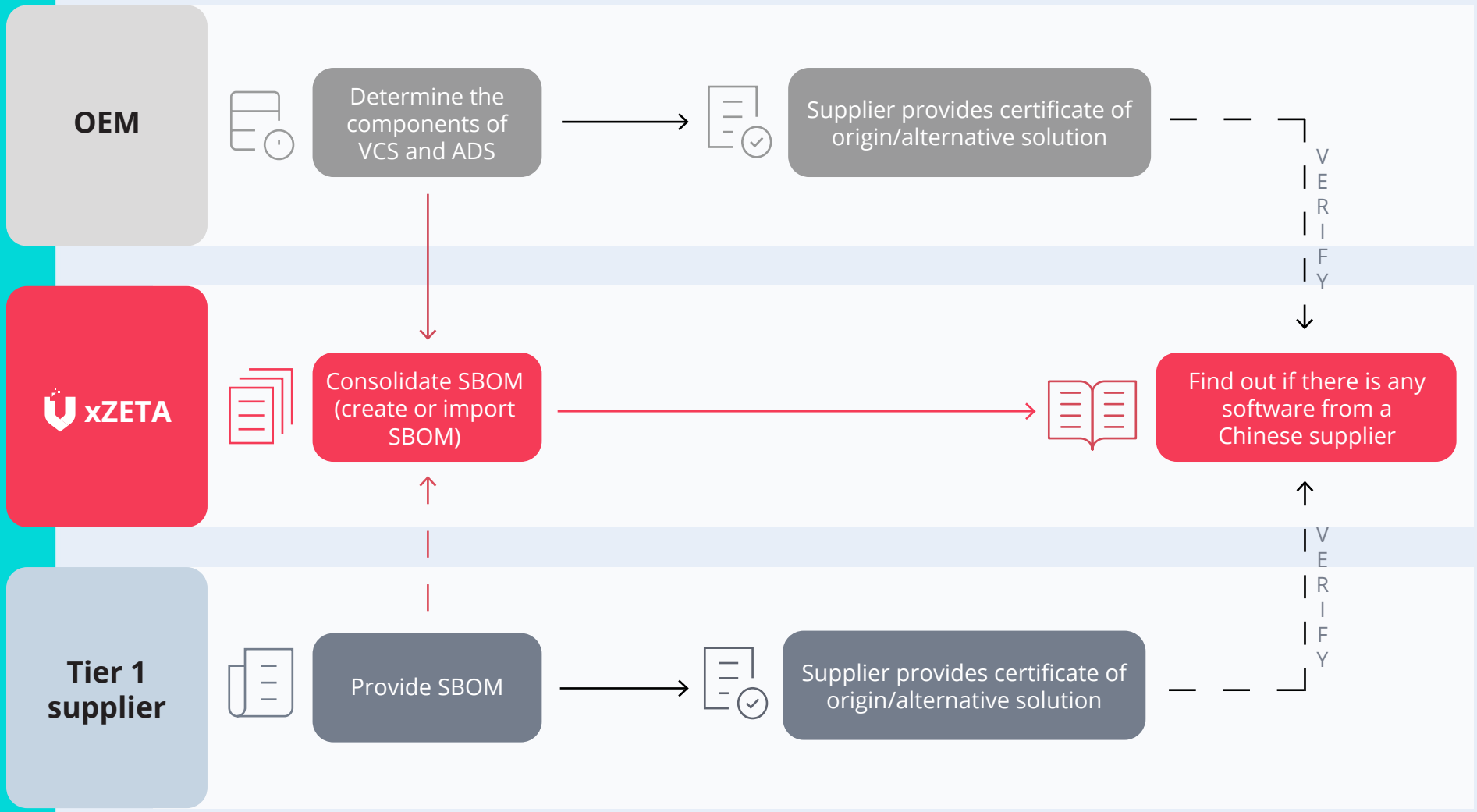




Problems:

- Manual process.
- Lack of visibility into the origins of software components.
- Data reflects only a single point in time.

But There's a Smarter Way: With xZETA, Software Origin Is Just One Click Away



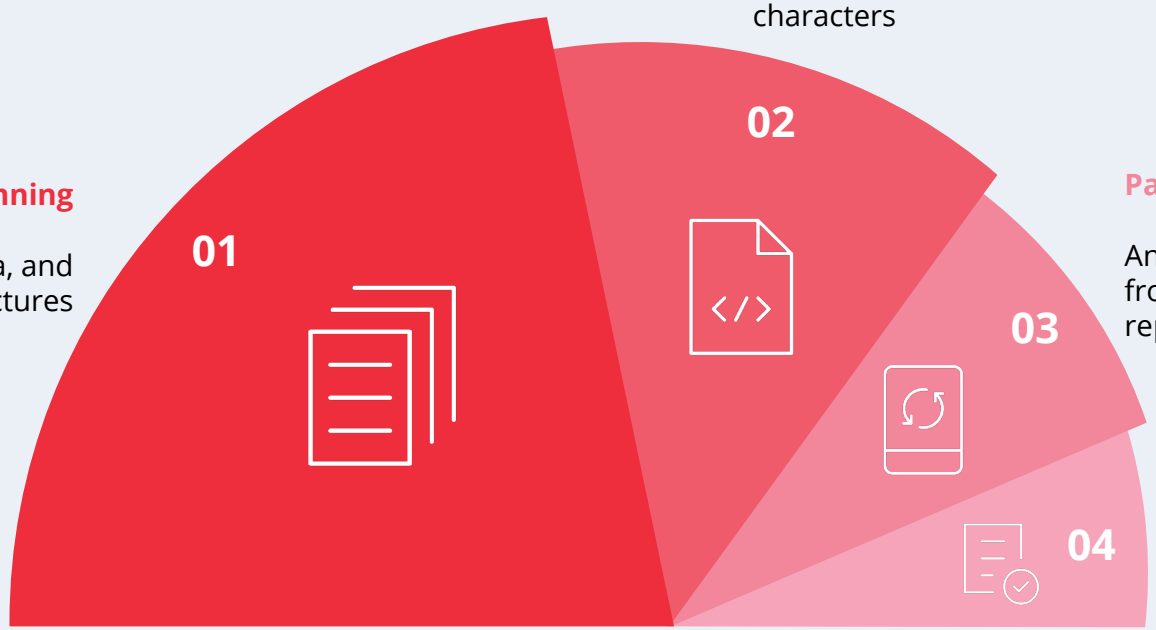
Superior Detection Capabilities

Multi-layer Scanning

Signatures, metadata, and structures

Encoding & Character Analysis

Identify encoding with Chinese characters



Pattern Recognition

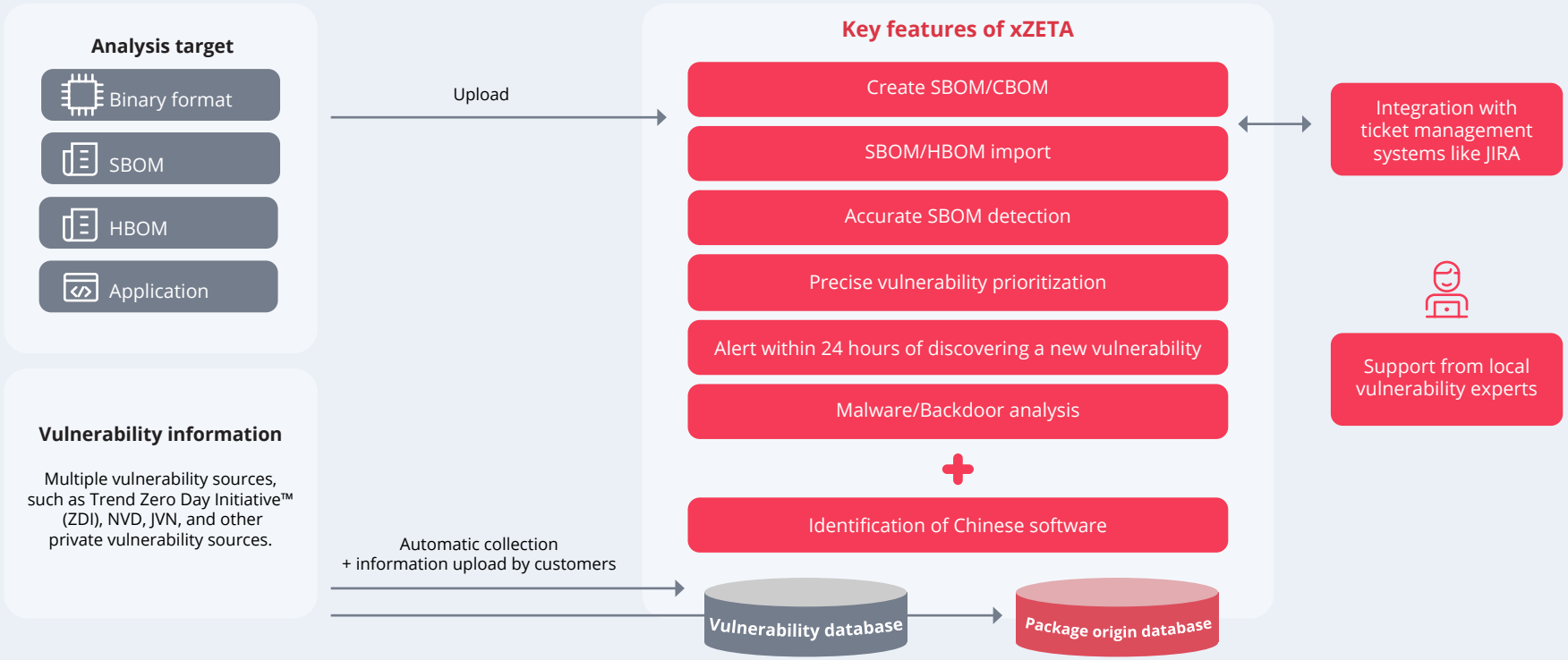
Analyzes package origin from URL domains and repository metadata

Sanction List Integration

OFAC, EAR, and custom blocklists

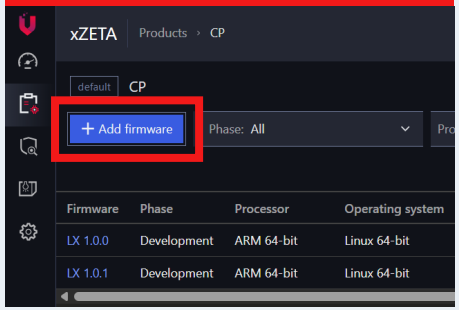
xZETA: Automotive Vulnerability and SBOM Management System

As a vulnerability and SBOM management tool tailored for the automotive industry, xZETA rapidly adapts to industry-specific needs and continuously updates features to keep pace with evolving requirements.

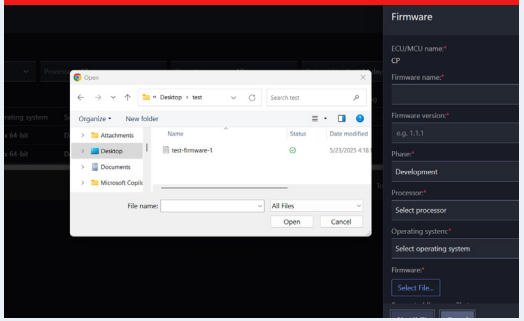


1. Generate an SBOM from firmware.

Click on “+ Add firmware”.



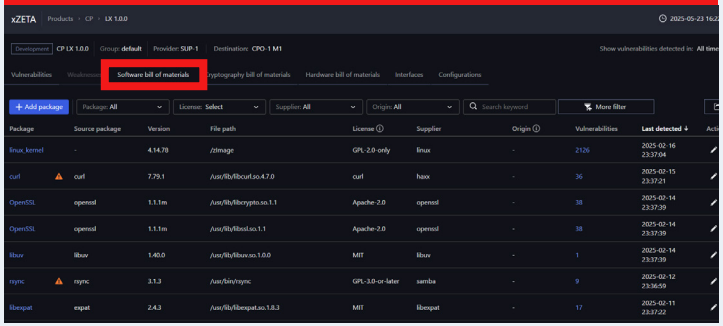
Configure the settings and select the file.



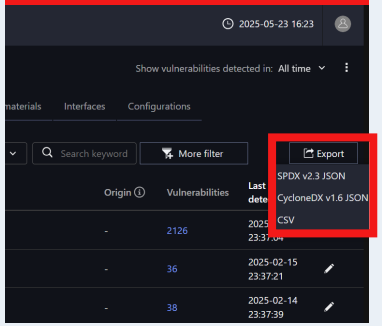
Quickly generate an SBOM just by uploading a binary.

Export the SBOM in SPDX or CycloneDX format as a JSON or CSV file.

The SBOM is successfully generated.

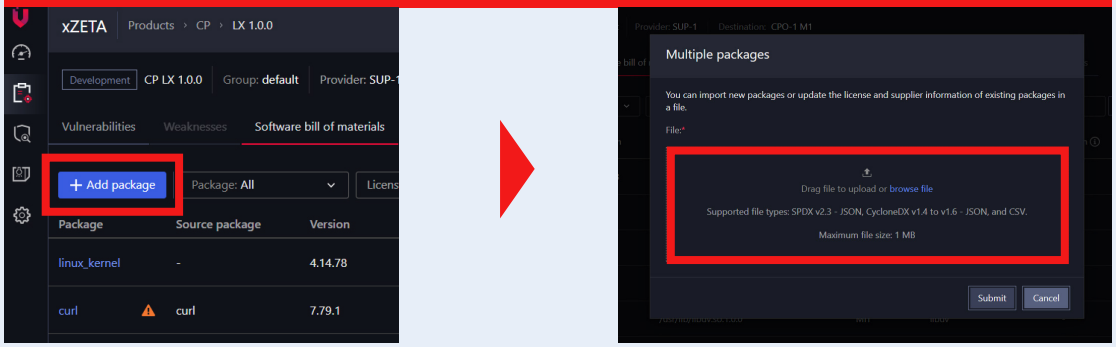


Choose the desired format and proceed to export.



2. If firmware is unavailable, import an existing SBOM.

Import multiple SBOMs via drag and drop.



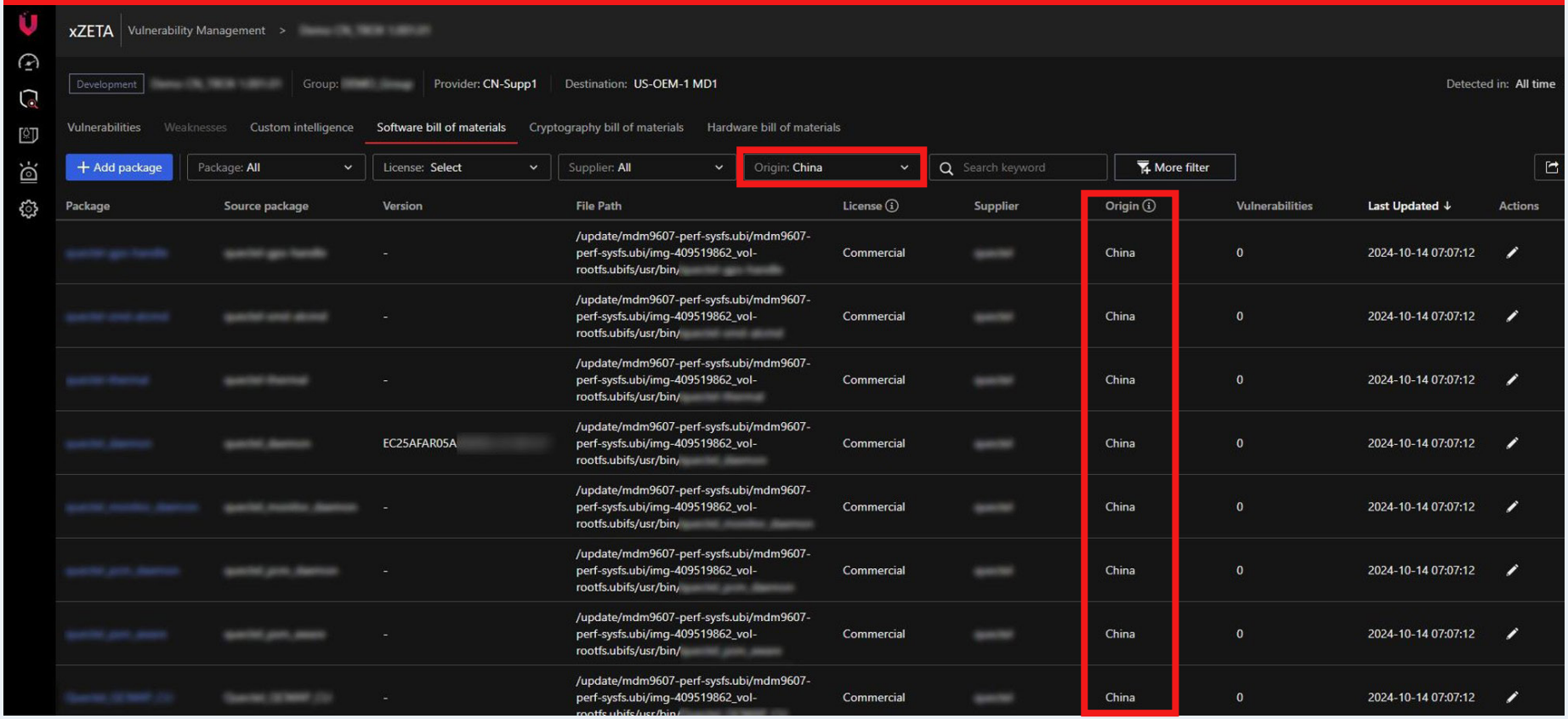
Add packages and edit the SBOM.

Edit the SBOM.

Package	Source package	Version	File path	License	Supplier	Origin	Vulnerabilities	Last detected	Acti
linux_kernel	-	4.14.78	/zImage	GPL-2.0-or Use commas to separate multiple licenses	linux	-	2126	2025-02-16 23:37:04	
curl	curl	7.79.1	/usr/lib/libcurl.so.4.7.0	curl	haxx	-	36	2025-02-15 23:37:21	
OpenSSL	openssl	1.1.1m	/usr/lib/libcrypto.so.1.1	Apache-2.0	openssl	-	38	2025-02-14	

3. Identify the software's country of origin — with one click.

Filter components by country of origin.



Your 3 Compliance Wins with xZETA

Quickly detect software origin changes before they turn into major risks.

Stay compliant with evolving U.S. regulations — no manual tracking needed.

Keep your product compliant and within standards from development to deployment.

VicOne

From Manual to One-Click

Identify Software's Country of Origin With xZETA

REQUEST A DEMO

xZETA

Learn more about VicOne by visiting VicOne.com or scanning this QR code: