Data Collection Disclosure

This page informs you of the data that is collected and transmitted by VicOne's security products, as part of providing you with the security functions of these products.

xZETA

xZETA is VicOne's cloud-based vulnerability management tool that scans vehicle software to identify potential security risks. It can detect known and undisclosed vulnerabilities in firmware. To deliver these functions, xZETA collects and processes certain categories of data as described below.

Data collection is categorized as:

- **Default Collection**: Data required for xZETA's core functions. These are required for platform operation and cannot be disabled.
- **Configurable Features**: Optional data collection that administrators can enable or disable based on operational needs.

Default collection

It is necessary to collect this data to provide the security functions of this product. Therefore, you cannot disable these features. If you do not want VicOne to access this data, you should stop using the product.

Feature	Data Collected	Configuration	Purpose
Firmware Scanning and Extraction	• Firmware information provided by the customer • ECU name, firmware name, firmware version number, OS name, OS architecture name, OS bit name • Software Bill of Materials (SBOM) • Name, version, path of the software in the firmware • Cryptography Bill of Materials (CBOM)	xZETA supports two modes of firmware information extraction. • SaaS mode: The xZETA Online Firmware Extractor sits inside the xZETA cloud environment. Firmware binary files are deleted immediately after extraction is completed. • Hybrid mode: The xZETA Hybrid Firmware Extractor is deployed to the customer's	Extract and analyze firmware components to identify security risks and provide vulnerability assessment

	• Certificates, private keys, secrets, digests • Hardware Bill of Materials (HBOM) • Processor codename • System context extracted by the Extractor • ELF information from libraries, kernel modules, and binaries • Kernel configuration • Information from startup services • Configurations of package manager data • Firewall configurations • System configurations • Scripts	environment. Only the extracted data are uploaded to xZETA. The firmware binary never leaves the customer's environment.	
General usage and audit logging	• Email addresses • IP addresses	-	Sign-in, onboarding, email notification delivery, and auditing

Configurable Features

The following features can be enabled or disabled by the customer. Disabling a feature stops the associated data from being collected and transmitted.

Feature	Data Collected	Configuration	Purpose
Single Sign-On	• Identity provider configuration and credentials	Administration > Single Sign-On	• Enable federated authentication through an external identity
Integrations	• Integration endpoint information and credentials	Administration > Integrations	• Enable integrations with external services

Data Controller & Privacy Contact

VicOne processes data as described above as data processor on behalf of its customers, on the basis of contract performance (Art. 6(1)(b)) and/or legitimate interests (Art. 6(1)(f)). For privacy inquiries or to exercise your data subject rights, contact **gdpr@vicone.com**. You also have the right to lodge a complaint with your local data protection authority.