Empowering Tomorrow's Automotive Software
www.etas.com

Automated vulnerability management **ESCRYPT CycurANALYZE** powered by ONEKEY

Enhanced security through effectively finding and triaging vulnerabilities in products

The digitalization of mobility is rapidly advancing, but this progress presents significant cybersecurity risks. **ESCRYPT CycurANALYZE powered by ONEKEY** addresses four major automotive industry challenges: rising vehicle connectivity and complexity amplify vulnerabilities, stringent regulations (e.g., UN-R155/156, ISO/SAE 21434) increase compliance pressure, complex supply chains introduce numerous potential weaknesses, and threats are dynamically increasing, shortening the time between vulnerability and security incident.

Areas of application

- Identification and management of vulnerabilities for automotive, embedded and IoT products to protect the integrity and safety throughout the lifecycle
- Finding vulnerabilities in key components such as the communication stack (both V2V and V2I) or in updating functionality (offline or FOTA)
- Management of security vulnerabilities e.g. in sensors, control units or telematics devices
- Supply chain transparency through continuous monitoring and implementation of Bill of Materials (BOM)

Features

- Software composition analysis by processing binary firmware or a BOM, e.g., CycloneDX
- Automated component identification from binaries through extraction, reconstruction, and detection of components, including version and license information
- Automated dependency mapping and creation of a comprehensive BOM that shows the relationships between components
- Continuous monitoring with real-time vulnerability scanning to map components against vulnerability databases such as NVD, and finding relevant CVEs and evaluations, e.g. CVSS, EPSS scores

Benefits

- **Comply with standards, and regulations:** ISO/SAE 21434, UN R 155, AIS 189, GB 44495, CRA
- **Be proactive in respective security strategies:** Save money by efficiently handling issues before they become security incidents
- **Think API-first:** Easily integrate the solution into the CI/CD pipelines for automated vulnerability management
- **Focus and prioritize:** Re-use existing Threat Analysis & Risk Assessment (TARA) for effective prioritization of vulnerabilities based on their context, reducing remediation time

Features and processes of vulnerability management

Creation of a Bill of Material (BOM)

Component identification from binaries

- Gain an accurate overview of software components in respective products
- Generate a comprehensive BOM directly from compiled binary files
- Identify components, versions, and license information

BOM verification

- Verify an existing BOM using a compiled binary file
- Detect hidden or undocumented dependencies of components, versions, and license information
- Identify whether a vendor has provided an incomplete or outdated BOM

Detection of vulnerabilities

Automated detection and prioritization

- Connection to internal or publicly available vulnerability databases like NVD
- Automatic mapping of BOM to available vulnerabilities by scanning BOM components against known vulnerabilities in your selected databases
- Categorization of vulnerabilities using the binary context

Improved software security

- Focus on source code and binary firmware with more than 40 scanners
- Track down command injection
- Find buffer overflow and other critical vulnerabilities
- Benefit from detailed reporting with recommended actions

Perfect combination to reduce risk and prioritize issues

Add-on: Risk-based vulnerability management

- Automatic prioritization of most critical vulnerabilities based on impact and context of assets by using ESCRYPT CycurRISK TARA information
- Accelerated decision-making with a strategic focus on most critical vulnerabilities
- The number of vulnerabilities in a product become more manageable, compared to scanning with a respective BOM without additional context
- Efficient capacity utilization by addressing issues that are most relevant in the product

Choose a specific solution to overcome security challenges

POSSIBILITIES

ETAS
Vulnerability Management as a Service
(VMaaS)

ETAS manages and delivers a comfort service

ETAS
Software as a Service
(SaaS)

ETAS manages the software, but users have access to it

ETAS
Software as a Product
(SaaP)

Users manage & have access to the software on-premise

Are you interested in ETAS products and solutions?
Please write to us at: **info@etas.com**

Further product information:
etas.com/vulnerability-management

ETAS/COM2_FS/03/2025