Empowering Tomorrow's Automotive Software
www.etas.com

ESCRYPT Intrusion detection and prevention solution

Efficient risk management for the entire lifecycle of vehicles

With the increasing connectivity of vehicles, new vectors for cyberattacks are emerging and attackers are constantly perfecting their methods. This erosion of security concerns all building blocks of a connected vehicle fleet: the vehicles themselves as well as the corresponding vehicle backend services.

As a result, maintaining the appropriate security for a connected fleet is a holistic and continuous activity. Detailed knowledge of the security status and potential attacks is paramount and required by upcoming regulations and standards. Consequently, a lifecycle approach is required which includes: Active security monitoring of the in-vehicle components and their communication, the fleet IT infrastructure and, finally, the automotive threat landscape as a whole.

Changing threat landscape

The threat landscape for connected vehicles is constantly evolving. Consequently, vehicle security degrades over time as attackers perfect their methods.

Mandatory regulations

Compliant cybersecurity management has become a decisive success factor for automotive managers. The UN Regulation 155 and the ISO/SAE 21434 standard mandate vehicle security for the entire lifecycle to receive type approval.

Our offering

ETAS offers an Intrusion Detection and Prevention Solution (IDPS) for connected fleets that enables OEMs to establish a lifecycle of permanent security monitoring and continuous adjustments.

Holistic end-to-end solution

The ESCRYPT IDPS solution for the automotive domain encompasses multiple in-vehicle IDPS software components and the ESCRYPT Vehicle Security Operations Center (VSOC) as a managed security service on the backend-side, which can be tailored to the specific needs of every customer environment. ETAS follows an open architecture concept with the IDPS; the solution components are also available as individual building blocks.

The ESCRYPT IDS sensors elicit security event information where it matters:

- Network-based intrusion detection for CAN and CAN FD with ESCRYPT CycurIDS-CAN
- Network-based intrusion detection for Ethernet with ESCRYPT CycurIDS-ETH
- Automotive Ethernet firewall with ESCRYPT CycurGATE
- Host-based intrusion detection especially for systems with rich operating systems and external interfaces

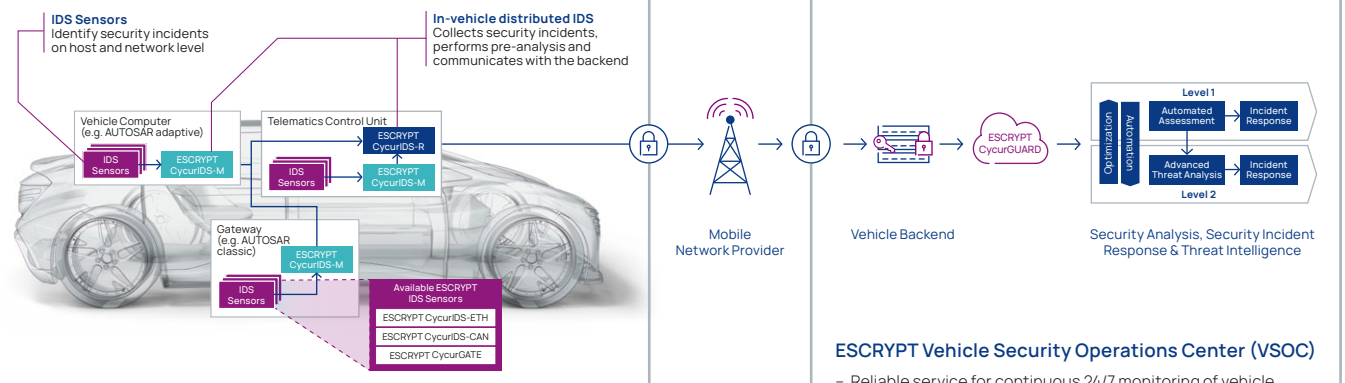
The ESCRYPT distributed IDS framework selects, persists and forwards the relevant security event information:

- ESCRYPT CycurIDS-M, in two variants:
  - for deeply embedded ECUs, i.e. µCs with classic AUTOSAR or RTOS
  - for larger platforms, i.e. µPs running adaptive AUTOSAR and/or some POSIX OS

  allows the management of security event information on ECUs, vehicle domains, or the complete vehicle. Compliant to the AUTOSAR IDS Manager (IdsM) specification, the ESCRYPT CycurIDS-M variants allow tailoring to any filtering, persistence, and reporting strategy.
- ESCRYPT CycurIDS-R for reporting of the security event information from the vehicle to the VSOC

The ESCRYPT Vehicle Security Operations Center enables fleet-wide monitoring:

- Unites all security event information sources from the vehicle fleets and vehicle backend systems, support of ESCRYPT CycurGUARD, ETAS' backend solution for onboarding security events
- Provides a complete vehicle security operations service from a single source



Distributed vehicle IDS architecture

- ESCRYPT CycurIDS-CAN, ESCRYPT CycurIDS-ETH and ESCRYPT CycurGATE act as smart sensors aggregating and pre-selecting potential security events (SEV) to enable a fast and correct analysis
- Host-based IDS for risk-based monitoring of ECUs
- ESCRYPT CycurIDS-M collects, analyses, aggregates, persists, and reports raised security events to the ESCRYPT CycurIDS-R
- ESCRYPT CycurIDS-R reports the security events from the vehicle to the VSOC

ESCRYPT Vehicle Security Operations Center (VSOC)

- Reliable service for continuous 24/7 monitoring of vehicle fleet security
- ESCRYPT CycurGUARD as security event onboarding backend
- Normalization and contextualization of detection reports
- Integration with OEM backend systems
- Security Analytics Service with automotive security forensic experts incl. threat detection & intelligence
- Analyst-validated and actionable security incident reports

Threat detection and threat intelligence

ESCRYPT CycurGUARD enables analysis of data from the entire connected fleet to identify emerging threats. With this monitoring backend product, ETAS offers an integrated solution for collecting and analyzing anomaly reports of vehicles in operation.

ESCRYPT CycurGUARD collects and preprocesses relevant data from a diverse set of data sources. It ensures that data from different domains (in-vehicle, infrastructure, backend services) is cross-referenceable so that the SIEM can use its full range of automated and manual detection capabilities.

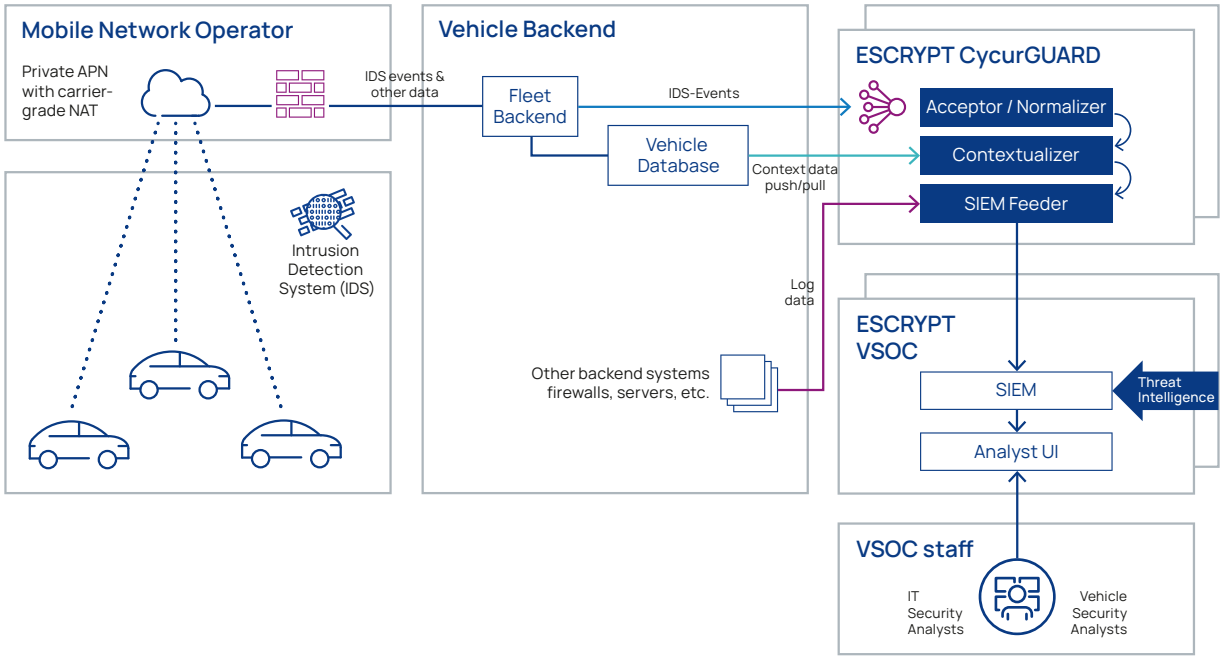
The VSOC reliably identifies acute threats referring to an extensive and continually growing database of known attack patterns, using ad-hoc or pre-built reports to help evaluating the safety and security of the connected fleet.

Specialized Automotive Security Forensic Experts take over the Incident Response process and Security Analytics. Leading IT security service providers support with comprehensive honeypot infrastructure and threat intelligence sources, which are combined with ETAS' automotive-specific public sources to establish a dedicated threat intelligence service.

Powerful partnership

ETAS cooperates with leading IT security service providers on the commissioning, infrastructure, and services of a security operations center (SOC). In this way, it pools the skills and expertise for SOC-as-a-Service with its own specialist automotive know-how and portfolio. We have taken the existing SOC infrastructure and expanded it with trained automotive security analysts and specialized forensics experts, turning it into a highly professional, market-ready, and holistic solution.

Our customers receive a vehicle security operations center as a managed security service that is perfectly adapted to the specific requirements of their connected fleet.



Your benefits

- Holistic offering that covers a complete distribution framework and sensors for in-vehicle intrusion detection (IDS) as well as a security monitoring backend and complementary SOC services
- Continuous monitoring of attacks in the field
- Timely detection of attacks
- Security analytics by forensic experts
- Enables rollout of countermeasures via updates for the entire fleet
- Delivery either as an end-to-end one-stop-solution tailored to the needs of the vehicle fleet or as individual components
- Compliant to AUTOSAR
- Enables compliance to legal requirements, e.g. UN Regulation 155

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

Weitere Produktinformationen:
www.etas.com/IDPS

ETAS/COM2_AS/12/2022