escrypt
SECURITY. TRUST. SUCCESS.

Vehicle Security Operations Center (V-SOC)

Overview

Increasing connectivity and automation of vehicles in combination with new regulations and standards like UNECE WP.29 and ISO/SAE 21434 will require OEMs and suppliers to monitor incidents and risks of their vehicle fleets over the entire life cycle. The threat landscape for connected vehicles is constantly evolving. Consequently, the security level of vehicles degrades over time as security measurements become ineffective and attackers learn to circumvent them. This erosion of the security level concerns all building blocks of a connected vehicle fleet: the vehicles themselves as well as the corresponding vehicle backend services. Detailed knowledge on the security status and potential attacks is paramount. Two activities establish this knowledge and keep it up to date:

Threat Detection

The timely detection and competent analysis of ongoing attacks is a key activity. With this fleet operators are able to take informed decisions and establish the appropriate measurements to restore the security level.

Threat Intelligence

The acquisition and collection of knowledge on known practicable attack patterns that may harm the security level of the connected vehicle solution.

ESCRYPT develops and operates a Vehicle Security Operations Center for connected fleets that enables manufacturers and fleet operators to establish a life cycle of continuous security improvements. This holistic solution ensures permanent monitoring to identify rising security threats, establish dedicated incident response, and keep the security level stable over the entire life cycle.

Customer challenges

- Continuously evolving threat landscape for vehicles
- Need to constantly maintain the security
- Scaling to vehicle fleets spread around the globe
- Fulfillment of upcoming worldwide regulations, such as UNECE WP.29 and ISO/SAE 21434

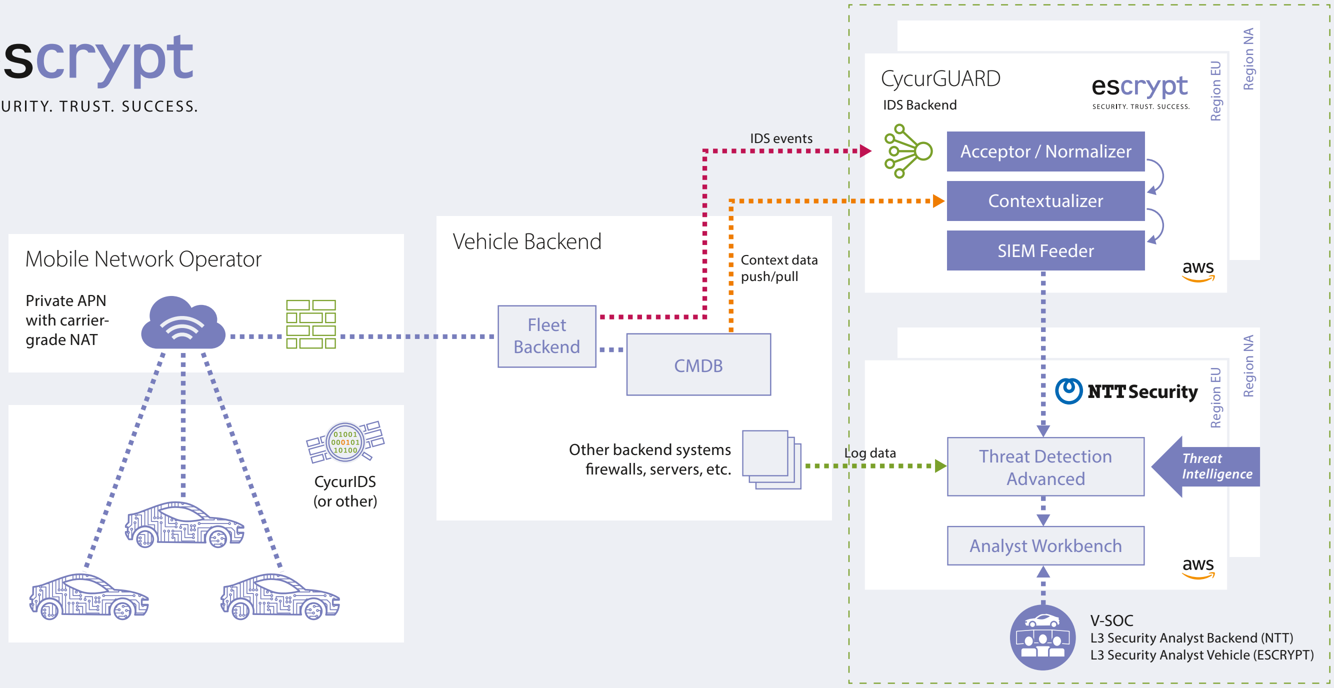
Our value proposition

- Holistic offering that covers in-vehicle intrusion detection (IDS) expertise with vehicle backend solutions and dedicated SOC services
- Continuous monitoring of attacks in the field by market-ready and mature ESCRYPT and NTT components
- Timely detection of attacks
- Security analytics by forensic experts
- Rollout of countermeasures via updates for the entire fleet

ESCRYPT 2020/10

escrypt

SECURITY. TRUST. SUCCESS.



Solution architecture

ESCRYPT delivers the Vehicle Security Operations Center (V-SOC) as a managed security service tailored to the needs of the vehicle fleet. This includes integration of event sources from the vehicle fleets and vehicle backend systems.

ESCRYPT's V-SOC follows an open architecture approach and integrates all sensors in the vehicle that provide information relevant for cybersecurity monitoring. This includes:

- Network-based intrusion detection for the CAN bus with ESCRYPT's CycurIDS
- Automotive Ethernet firewalls with ESCRYPT's CycurGATE
- Host-based intrusion detection for Linux, QNX, and Android ECUs
- Support for the complex distributed IDS architectures of modern E/E architectures

The V-SOC consists of the following components:

V-SOC: Security Operations Center services

ESCRYPT collaborates with NTT Security, the leading Security Operations Center (SOC) services provider worldwide. This partnership unites NTT's operational excellence and expertise in the area of SOC as a service with ESCRYPT's automotive security know-how and provides customers with a highly professional and truly holistic solution that covers in-vehicle and backend security. The benefits:

- Worldwide availability: 10 SOCs with 24/7 operation
- Multi-regional rollout: one solution to cover all regions with 600+ security experts
- Highly recognized: battle-proven SOC tooling and infrastructure

V-SOC: Threat detection

ESCRYPT's CycurGUARD enables analysis of data from the entire connected fleet to identify emerging threats. With the monitoring backend product based on big data analysis technologies, this component collects and analyzes anomaly reports of vehicles in operation:

- Interlocking of automated and manual analysis:
  - Automatic classification of events and automated processing of known attack patterns
  - Manual alert validation by teams of automotive security forensic experts to identify emerging threats
- Event-based threat hunting
- Actionable incident notification with recommendations
- Incident support until resolution is achieved
- Proactive response with network threat containment

V-SOC: Threat intelligence

- Comprehensive honeypot infrastructure
- Access to dedicated automotive-specific public sources
- More than 10 Enterprise IT threat intelligence sources

V-SOC: Data privacy and compliance

ESCRYPT's V-SOC backend correlates security event information on the basis of pseudonyms instead of personal data such as the vehicle identification number (VIN). Pseudonymization is an integral part of the solution.

ESCRYPT is a pioneer and leading provider of IT security solutions in the automotive sector. By developing software applications and providing extensive consulting services, it has been protecting vehicles for over 15 years.