escrypt
SECURITY. TRUST. SUCCESS.

Vehicle Security Operations Center

Überblick

Die Gefahrenlandschaft für vernetzte Fahrzeuge entwickelt sich ständig weiter. Die Nodwendigkeit für eine umfassendere Security betrifft nicht nur die Autos selbst, sondern auch die entsprechenden Backend-Dienste und damit alle Komponenten einer vernetzten Flotte.
Die Sicherheit der Fahrzeuge kann nur durch einen ganzheitlichen und fortlaufenden Prozess auf dem entsprechenden Niveau gehalten werden. Detaillierte Daten über den Sicherheitsstatus und potenzielle Angriffe sind dabei nicht nur technisch unabdingbar, sondern werden auch von neuen Regulierungen und Normen gefordert. Sie lassen sich durch zwei Verfahren erfassen und pflegen:

Bedrohungserkennung: Im Zentrum steht die rechtzeitige Erkennung und korrekte Analyse laufender Angriffe. Dank der so erfassten belastbaren Informationen lassen sich fundierte Entscheidungen treffen und die Sicherheit durch geeignete Maßnahmen wiederherstellen.

Threat Intelligence: Dieses Verfahren liefert Erkenntnisse zu neuen Angriffsmustern und Angriffstechniken.

ESCRYPT entwickelt und betreibt ein Vehicle Security Operations Center (Vehicle SOC) für vernetzte Flotten, mit dem Hersteller und Flottenbetreiber die Sicherheit ihrer Fahrzeuge kontinuierlich über den gesamten Lebenszyklus hinweg verbessern können.

Herausforderungen unserer Kunden

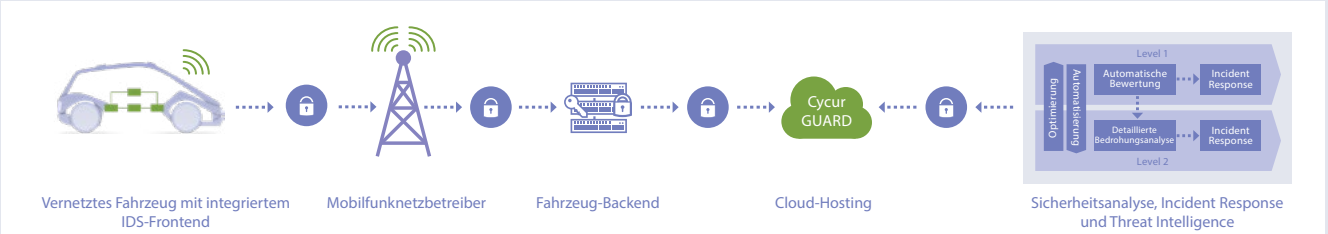
- Ständige Veränderungen in der Gefahrenlandschaft für Fahrzeuge und damit verbundene passende Response.
- Gleichbleibend hohes Sicherheitsniveau
- Skalierbarkeit für weltweit aktive Fahrzeugflotten
- Erfüllung neuer weltweit geltender Vorgaben wie UNECE WP.29 und ISO/SAE 21434

Unsere Lösung

- Ganzheitlicher Security-Ansatz mit fahrzeugintegriertem Angriffserkennungssystem (IDS) sowie Fahrzeug-Backend
- Lückenlose Angriffsüberwachung im Fahrzeugbetrieb
- Frühzeitige Angriffserkennung
- Sicherheitsanalysen durch Forensiker
- Rollout wirksamer Gegenmaßnahmen durch Updates für die gesamte Flotte

ESCRYPT 07/2020

escrypt
SECURITY. TRUST. SUCCESS.



Vernetztes Fahrzeug mit integriertem IDS-Frontend | Mobilfunknetzbetreiber | Fahrzeug-Backend | Cloud-Hosting | Sicherheitsanalyse, Incident Response und Threat Intelligence

IDS-Architektur für Fahrzeug

- Alle Komponenten der Angriff serkennung (CycurIDS, CycurGATE) speziell für den Automobilbereich
- Kenntnis von Fahrzeugnetzen und Angriffsvektoren
- Integrationskomponenten für verteilte IDS
- Konfigurationsservice für IDS

Komplettlösung für Kunden

- CycurGUARD mit IDS-Bausteinen für den Einsatz im Fahrzeug
- Kontextualisierung von Angriffs- berichten
- Integration in Backend-Systeme von OEMs
- Pseudonymisierung für sicheren Datenschutz

Security Operations Center Services

- Sicherheitsanalysedienst mit Foren- sikern aus der Automotive Security
- Bedrohungserkennung und Threat Intelligence: Zehn rund um die Uhr aktive SOCs weltweit
- Services für Fahrzeugflotten wie auch Enterprise IT

Benefits

Ganzheitliche Komplettlösung für optimalen Schutz

ESCRYPT bietet das Vehicle SOC als Managed Service an, der auf die Bedürfnisse der jeweiligen Flotte zugeschnitten ist. Dies beinhaltet auch die Integration von Ereignisquellen aus den Fahrzeugflotten und -Backend-Systemen.

IDS-Architektur für Fahrzeuge

Das Vehicle SOC von ESCRYPT setzt auf eine offene Architektur und bindet sämtliche Fahrzeugsensoren ein, die relevante Daten für die Überwachung der Cybersicherheit liefern. Das Leistungs spektrum umfasst:

- Netzwerkbasierte Angriffserkennung am CAN-Bus dank CycurIDS von ESCRYPT
- Automotive Ethernet Firewalls durch CycurGATE von ESCRYPT
- Host-basierte Angriffserkennung für Linux-, QNX- und Android-Steuergeräte
- Support für komplexe verteilte IDS-Architekturen moderner E/E-Architekturen

Security Operations Center (SOC) Services

ESCRYPT kooperiert mit dem Branchenexperten NTT Security, dessen führende SOC-Services zahlreiche Kunden weltweit nutzen. So bietet ESCRYPT seinen Kunden eine hochprofessionelle, ganzheitliche Lösung, die sowohl Fahrzeug als auch Backend schützt. Entstanden ist sie aus der Symbiose der operativen Exzellenz und dem Know-how rund um SOC-as-a-Service von NTT Security einerseits und der Automotive-Security-Expertise von ESCRYPT andererseits. Die Vorteile:

- 10 SOCs von NTT im 24-Stunden-Betrieb garantieren eine weltweite Verfügbarkeit
- Überregionaler Rollout dank einheitlicher Lösung für alle Regionen mit über 600 Sicherheitsexperten
- Bewährte SOC-Tools und -Infrastrukturen

Bedrohungserkennung

- Moderne Analysefähigkeiten mit Machine Learning und Modellierung des Bedrohungsverhaltens
- Automatische Validierung von Warnmeldungen mittels Künstlicher Intelligenz bei bekannten Angriffsmustern
- Manuelle Validierung durch Sicherheitsanalysten bei neuen Bedrohungen
- Ereignisbasierte Bedrohungssuche
- Aussagekräftige Vorfallbenachrichtigung mit Empfehlungen
- Unterstützung bei Vorfällen bis zu deren Lösung
- Proaktive Maßnahmen mit Eindämmung der Netzwerkbedrohung

Threat Intelligence

- Umfassende Honeypot-Infrastruktur
- Rückgriff auf SOCs und Backends von NTT Security mit Abdeckung von 40 % des Datenaufkommens weltweit
- Über zehn Threat-Intelligence-Quellen

Datenschutz und Compliance

Die Pseudonymisierung von Daten ist zentraler Bestandteil des Konzepts: So erfasst das Vehicle SOC von ESCRYPT Informationen zu Sicherheitsereignissen anhand von Pseudonymen statt persönlichen Daten wie der Fahrgestellnummer.

ESCRYPT ist Vordenker sowie führender Anbieter für IT-Security-Lösungen im Automobilsektor und bietet seit über 15 Jahren selbstentwickelte Softwareanwendungen und umfangreiche Beratungsservices für den ganzheitlichen Fahrzeugschutz. Heute sind ESCRYPT-Lösungen vielerorts Bestandteil der automobilen Serienproduktion und in Millionen Fahrzeugen weltweit im Einsatz.