Umfassende Testservices zur Vermeidung von Automotive Cyberangriffen.

www.tuv.com/informationssicherheit

TÜVRheinland®
Genau. Richtig.

Mit fortschreitender Digitalisierung wird auch die Fahrzeugausstattung smarter: Von Bedienfeldern über MRO-Programme bis hin zum klassischen GPS enthalten Fahrzeuge eine erhebliche Anzahl smarter Funktionen. Wie smarte Produkte wird auch das vernetzte Fahrzeug zum Ziel von Cyberangriffen.

WELCHES AUSMASS HABEN CYBERANGRIFFE AUF KRAFTFAHRZEUGE?

Die Bedrohungen reichen von der einfachen unbefugten Datenerfassung bis hin zu schwereren Vergehen wie Fahrzeug- oder Eigentumsdiebstahl, böswilliger Entführung oder gar der Möglichkeit der Außerkraftsetzung wichtiger Systeme und Steuerungen per Fernzugriff mit Unfall-, Verletzungs- oder gar Todesfolge.

WELCHER ANSATZ WIRD ZUR VERMEIDUNG VON ANGRIFFEN VERFOLGT?

Durch die strategische Partnerschaft zwischen TÜV Rheinland und VisualThreat erweitern wir unsere Leistungen zur Vermeidung von Cyberangriffen in Fahrzeugen und erhöhen damit letztlich die Sicherheit der nächsten Fahrzeuggeneration. Wir unterstützen die Automobilindustrie dabei, Sicherheitsangriffe auf die nächste Fahrzeuggeneration sowie die Fahrzeugkommunikationsnetzwerke zu testen, zu erkennen und zu verhindern. Mit den Testeinrichtungen und der Erfahrung von TÜV Rheinland und der Cyber-Security-Technologie von Visual Threat stehen der Automobilbranche und den Zulieferern umfassende Testservices zur Verfügung, die Ihren Produkten einen guten Schutz gegen zukünftige Cyberangriffe bieten und Branchenstandards in Bezug auf einen sicheren Betrieb erfüllen.

TEST- UND CYBER-SECURITY-EINRICHTUNGEN MIT GROSSER ERFAHRUNG

TÜV Rheinland unterstützt seit mehr als 15 Jahren den privaten und öffentlichen Sektor mit umfassender Beratungs- und Lösungskompetenz in den Bereichen IT, Cyber Security und Telekommunikation bis hin zu digitalen Transformationsprozessen. Mit weltweit mehr als 600 Experten bietet TÜV Rheinland strategische Beratung, Design- und Prozessoptimierung bis hin zu Implementierung, Betrieb und Zertifizierung von Systemen. Übrigens: TÜV Rheinland prüft als eine der weltweit ersten autorisierten Organisationen Informationssicherheit nach TISAX.

VISUALTHREAT ALS STRATEGISCHER PARTNER

VisualThreat ist ein führender Anbieter von Cyber-Security-Tests im Automotive Bereich mit Sitz in Kalifornien und stellt umfassende Fahrzeugsicherheitslösungen zur Abwehr von Cyberangriffen bereit. Das Auto Cyber Security Testing Lab bietet Sicherheitspenetrationstests für OEMs und Zulieferer an. In den letzten Jahren hat VisualThreat OEMs und Zulieferer dabei unterstützt, die Sicherheitsfunktionen in Fahrzeugen zu verbessern. Das Testlabor des Unternehmens bietet einen automatischen Cyber-Security-Testrahmen für Kraftfahrzeuge an.

Das Automotive Cyber Security Testing Framework von VisualThreat umfasst mehr als 30 Prüfpunkte aus folgenden Kategorien: CAN Bus Probing, Testen einzelner Steuergeräte sowie CAN-Kommunikationsprüfung für mehrere Steuergeräte. Die Tests können entweder lokal oder über Cloud-basierte Modi durchgeführt werden.

TÜV Rheinland
ICT & Business Solutions
Am Grauen Stein
51105 Köln
Tel. +49 221 806-0
service@i-sec.tuv.com

www.tuv.com/de/automotive-sec

VisualThreat
Make cars Secured and Connected

TÜVRheinland®
Genau. Richtig.