Complete testing services for the prevention of automotive cyberattacks.

www.tuv.com/informationsecurity

TÜVRheinland®
Precisely Right.

With advances in digitization, vehicle equipment becomes smarter as well: from control panels over MRO programs to classic GPS – vehicles contain a significant number of smart functions. Like smart products the connected car becomes a target for cyberattacks.

WHAT IS THE EXTENT OF AUTOMOTIVE CYBERATTACKS?

Threats range from simply unauthorized data capture to more serious offenses such as vehicle or property theft, criminally malicious hijacking or even the possibility of remotely overriding critical auto systems and control, resulting in accident, injury, or even death.

WHAT IS THE APPROACH FOR ITS PREVENTION?

Through the strategic partnership between TÜV Rheinland and VisualThreat, we will deepen our services to prevent cyberattacks in vehicles and ultimately increase the safety of next generation vehicles on the roads. We aim at helping the automotive industry test, detect and remediate the increasing cyber security threats targeting next generation vehicles and vehicle communication networks. TÜV Rheinland's testing facilities and experience and VisualThreat's cyber security technology will provide automotive industry and component manufacturers with complete testing services to ensure their products are secure from cyberattacks and meet industry standards for secure performance.

EXPERIENCED TESTING & CYBER SECURITY FACILITIES

TÜV Rheinland has been supporting the private and public sector with comprehensive consulting and solution expertise in IT, cyber security and telecommunications through digital transformation processes for more than 15 years. With more than 600 specialists around the world, TÜV Rheinland provides strategic consulting, design and process optimization through to implementation, operation, and certification of systems. At the beginning of 2017, we opened a state-of-the-art internet of things (IoT) excellence center in Fremont, California. The new facility provides manufacturers complete testing services, supported by state-of-the-art equipment, to ensure their products are secure and meet industry standards for performance. By the way: TÜV Rheinland audits Information Security controls in accordance with TISAX as one of the first authorized organizations worldwide.

VISUALTHREAT AS STRATEGIC PARTNER

VisualThreat is a leading automotive cyber security testing vendor based in California, offering the end-to-end automotive security solutions to minimize penetration from cyberattacks. The Auto Cybersecurity Testing Lab offers security penetration testing services for OEMs and tier providers. For the past years, VisualThreat has helped OEMs and tier providers enhance security functions inside vehicles. The company testing lab offers an automatic automotive cyber security testing framework for vehicles

VisualThreat's Automotive Cyber Security Testing Framework contains more than 30 testing checkpoints from the following categories: CAN bus probing, individual ECU testing, and CAN communication testing among several ECUs. The testing can be performed either by local or via the cloud based modes.

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

www.tuv.com/en/automotive-sec

VisualThreat
Make cars Secured and Connected

TÜVRheinland®
Precisely Right.