# Runecast Extends AI-powered Security Compliance to TISAX Standard for German Auto Industry

Runecast's AI-powered vulnerability management and security compliance capabilities extend to the German automotive industry's TISAX standard.

LONDON, UNITED KINGDOM, April 4, 2023 /EINPresswire.com/ -- Runecast Solutions Ltd., a leading provider of a cloud-native application protection platform (CNAPP) for AI-powered automation of vulnerability management, security compliance, container security and more efficient ITOM, is pleased to announce that its April release adds coverage for the German automotive industry's TISAX security standard.

Runecast helps the German automotive industry with TISAX compliance
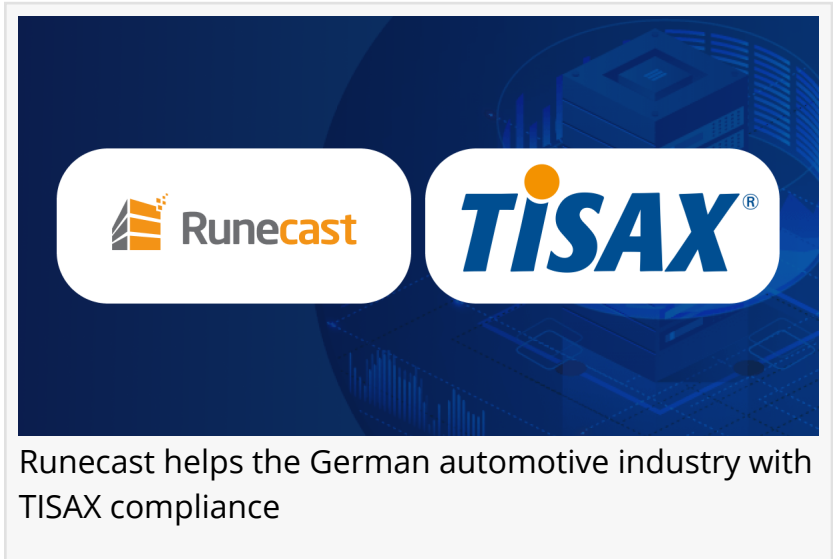
TISAX, for Trusted Information Security Assessment Exchange, is a security standard developed by the German Association of the Automotive Industry (Verband der Automobilindustrie, or VDA) to secure the German automotive industry. Audits for the TISAX standard will be available to Runecast customers in the upcoming release, aimed for mid-April.

> Runecast automates compliance checks against TISAX to help organizations ensure a high level of information security across their supply chain, while minimizing the time and resources required."
> *Markus Strauss, Chief Product Officer at Runecast*

"We are pleased to add TISAX to the growing list of standards for which we provide customers with automated, continuous compliance," said Markus Strauss, Chief Product Officer at Runecast. "Runecast automates compliance checks against the TISAX standard to help organizations ensure a high level of information security across their supply chain, while minimizing the time and resources required, and increasing the effectiveness of their compliance process."

SECURITY FOR SAFER AUTOBAHNS
A [report from ENISA](#), the European Union Agency for Cybersecurity, concludes that ransomware is the top threat to the European transportation network. On March 20, 2023, [Ferrari announced](#) that it had suffered a ransomware attack compromising its customers' sensitive personal information.
While having some overlap with the better-known ISO/IEC 27001 standard for IT security management, TISAX adds specific requirements for the automotive sector – an area in which successful cyber attacks can be fatal and data breaches are made increasingly possible by interconnected vehicle systems.

Like GDPR, in which multinational companies are required to adhere to a European standard when doing business with Europeans, the requirement for TISAX certification applies to any multinational automotive suppliers that wish to have or continue doing business with German automotive companies.

RUNECAST PUTS TISAX COMPLIANCE ON AUTOPILOT
[Recommended by CISA](#) (the US Government's Cybersecurity and Infrastructure Security Agency), Runecast was one of the first security platforms to integrate with the CISA Known Exploited Vulnerabilities (KEVs) catalog. Using Runecast AI Knowledge Automation (RAIKA), Natural Language Processing (NLP), OpenAI integration and a patented rules engine (US Patent No. US-10621234-B2), Runecast provides proactive discovery of vulnerabilities, misconfigurations, and any non-compliance with security standards and vendor best practices. Built-in audits against the CISA KEV catalog are a key ingredient in prioritizing remediation efforts based on risk – to help security teams daily prioritize discovered issues.

For companies in the automotive supply chain seeking help in automating TISAX assessments and compliance, Runecast's AI-powered platform provides automated vulnerability assessments and security compliance auditing along with simple steps to remediate any discovered issues like misconfigurations or non-compliances.

In addition to TISAX coverage, built-in audits for compliance with specific security standards include BSI IT-Grundschutz, CIS Benchmarks, GDPR, ISO 27001, NIST and others, for on-premises, hybrid and multi-cloud environments.

"Our German customers already include the German Aerospace Center (DLR), Helmholtz Zentrum für Materialien und Energie GmbH and, for example, large enterprises in the pharmaceutical and aeronautical software industries," said Mr. Strauss, "so we are glad to help improve the security posture of companies also in the automotive industry."

Runecast innovation stands to be a key efficiency enabler for helping with TISAX compliance, for companies that include:

– Bayerische Motoren Werke (BMW) AG (incl. BMW Motorrad, BMW Motorcycles, MINI, Rolls-

Royce);

– Daimler AG (incl. Mercedes-AMG, Mercedes-Maybach, Smart);

– Ford-Werke GmbH;

– Opel Automobile GmbH (part of French PSA Group and Dutch Stellantis N.V., which owns Abarth, Alfa Romeo, Chrysler, Citroën, Dodge, DS, Fiat, Fiat Professional, Jeep, Lancia, Maserati, Mopar, Peugeot, Ram, Vauxhall);

– Volkswagen AG (incl. Audi, Bentley, Cupra, Lamborghini, Porsche, SEAT, Škoda, Volkswagen, Ducati motorcycles, Volkswagen Commercial Vehicles, Traton, Navistar, MAN, Scania, Volkswagen Truck & Bus);

– Germany-based auto parts manufacturers

– Any multinational automotive company (such as parts suppliers) doing business with German automotive companies.

Runecast customers report between 75-90% time savings in the areas of troubleshooting, upgrade planning and the ability to achieve, maintain and verify security compliance. It enables IT security teams with far greater efficiency, resulting in cost savings, operational transparency, and continuous compliance. The platform helps organizations stay ahead of potential security threats and maintain compliance with industry standards.

Jason Mashak
Runecast Solutions Ltd.
email us here
Visit us on social media:
Twitter
LinkedIn

This press release can be viewed online at: https://www.einpresswire.com/article/626011485