When cyber risks cross company boundaries

AI-related threats, complex supplier networks and faster software updates are changing automotive cybersecurity. For legacy products, contracts may not clearly define who is responsible for security patches.

Discuss your challenge wth Mirko Ross



CHALLENGES AUTOMOTIVE DECISION-MAKERS ARE FACING

- » AI as an accelerator of emerging cyber threats
- » Unclear responsibilities across OEM and supplier environments
- » Software update cycles that differ across supplier networks
- » Legacy products where patch responsibilities are not clearly defined

HOW ASVIN CAN CONTRIBUTE

asvin applies Cyber Risk Management and Cyber Threat Intelligence to help organizations understand relevant threats and risks in their specific context.

AI supports this work as an accelerator of analysis, and is also considered as a factor changing the threat landscape.
In an initial conversation, we explore whether asvin's expertise fits your organization's challenge.

A JOINT AUTOMOTIVE USE CASE

DXC Technology / DXC Luxoft and **asvin** connected vehicle-level security events with Cyber Threat Intelligence. The CTI capability used in this specific use case also underlies CTI HORIZON™.

Read the DXC and asvin case study ↗



CUSTOMERS & PARTNERS

Volkswagen | Customer

Bertrandt | Partner

Capgemini | Partner

Capgemini | Partner

Mirko Ross
CEO & Co-Founder

In an initial conversation, explore whether asvin may be able to support a challenge affecting your OEM organization.

Contact Mirko Ross

asvin gmbh | Eichwiesenring 1/1 | 70565 Stuttgart
contact@asvin.io | asvin.io/automotive-cybersecurity/