

VicOne and CYMETRIS Turn New CVEs into Vehicle-Specific Risk Decisions as AI Accelerates Vulnerability Discovery

Bidirectional integration connects automotive vulnerability intelligence with system-level risk engineering, bringing Live TARA to automotive risk modeling.

MUNICH, MUNICH, GERMANY,

September 23, 2026 /

EINPresswire.com/ -- VicOne, [a Japan-headquartered leader in automotive and physical AI cybersecurity](#), and

CYMETRIS, a cyber risk engineering platform provider, today announced an integration of [VicOne xZETA](#) and the CYMETRIS platform. It helps automotive OEMs and suppliers

identify which newly disclosed vulnerabilities matter to a specific vehicle program, understand their potential impact in the vehicle architecture, and revisit risk decisions as software and threats change.



Connecting xZETA's automotive-specific intelligence with CYMETRIS' system-level risk model helps teams move from a new finding to a defensible treatment decision."

Max Cheng, Chief Executive Office, VicOne



VicOne and CYMETRIS Turn New CVEs into Vehicle-Specific Risk Decisions as AI Accelerates Vulnerability Discovery

Across the broader software ecosystem, serious vulnerability disclosures are climbing. In [an analysis by Luke Emberson for Epoch AI](#), 21 major technology organizations disclosed approximately 2,500 high- and critical-severity CVEs in July 2026, about 60% more than in June and roughly five times the monthly high recorded before April 2026. As AI-assisted vulnerability discovery advances, automotive product security teams face a pressing question: Which findings actually affect their vehicles? Answering it requires connecting vulnerability intelligence with software bills of materials (SBOMs),

vehicle architectures, and TARA records, work that still often depends on spreadsheets, tickets, and manual handovers.

The integration puts Live TARA into practice at the automotive risk-model layer. Live TARA describes an approach to keeping Threat Analysis and Risk Assessment (TARA) current as vulnerabilities, vehicle software, and system architectures change. VicOne xZETA supplies continuous automotive vulnerability and SBOM intelligence. CYMETRIS evaluates relevant findings against the actual vehicle architecture so that affected attack paths, controls, damage scenarios, and risk ratings can be reassessed.

Through a bidirectional API bridge, xZETA sends relevant findings to linked CYMETRIS projects. CYMETRIS relates them to affected assets and electronic control units (ECUs), assesses whether existing controls could be circumvented, and maintains a traceable record of resulting treatment decisions. Architecture context also flows back to xZETA, enabling findings to be evaluated against the system model rather than a flat component list.

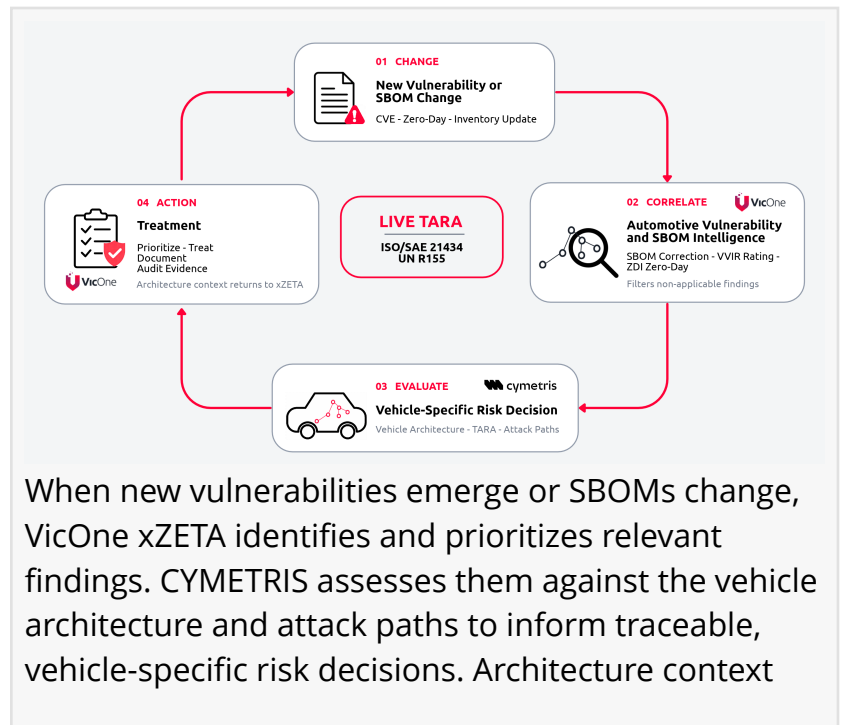
When new vulnerabilities emerge or SBOMs change, VicOne xZETA identifies and prioritizes relevant findings. CYMETRIS assesses them against the vehicle architecture and attack paths to inform traceable, vehicle-specific risk decisions. Architecture context then flows back to xZETA, keeping the assessment current.

“Automotive organizations do not need more vulnerability alerts. They need to know which findings can affect a specific vehicle and what to do next,” said Max Cheng, Chief Executive Office, VicOne. “Connecting xZETA’s automotive-specific intelligence with CYMETRIS’ system-level risk model helps teams move from a new finding to a defensible treatment decision.”

VicOne xZETA generates and maintains SBOMs in standard formats and identifies vulnerabilities beyond generic CVE feeds. Its VicOne Vulnerability Impact Rating (VVIR) helps prioritize findings using the customer’s software inventory and automotive context, supported by VicOne research and zero-day intelligence from TrendAI™ Zero Day Initiative™ (ZDI).

CYMETRIS maps assets, threats, attack paths, and controls to system architecture. Its platform supports visual attack-path analysis, circumvent-path modeling, continuous risk analysis, and vertical TARA collaboration between OEMs and suppliers.

“Risk cannot be determined by a severity score alone,” said Falk Mayer, Co-Founder and



Managing Director, CYMETRIS. “A vulnerability becomes meaningful when organizations can see where it exists, whether it is reachable, which controls could be bypassed and what damage could result. This integration gives engineering and PSIRT teams that shared context without requiring manual handovers between disconnected tools.”

For automotive OEMs and suppliers, the combined workflow helps:

- Filter non-applicable vulnerabilities before they reach engineering teams.
- Identify affected vehicle programs, ECUs, attack paths and damage scenarios.
- Assess whether existing controls could be circumvented.
- See where shared components appear across multiple vehicle programs.
- Maintain a documented basis for prioritization and treatment decisions.
- Align PSIRT and cybersecurity engineering around one consistent data model.
- The integration also supports evidence management for ISO/SAE 21434 and UN R155 activities.

When a relevant vulnerability or architecture change occurs, organizations can update and version the risk model while retaining traceability across development, start of production and field operations.

VicOne and CYMETRIS will jointly demonstrate the integration at two upcoming events in Germany: ELIV 2026, taking place October 14–15 in Baden-Baden, and it-sa Expo&Congress 2026, taking place October 27–29 in Nuremberg. Attendees can experience the integration at it-sa in Hall 7, Booth 7-402.

About CYMETRIS

CYMETRIS, headquartered in Munich, Germany, is a software company for cybersecurity risk management in product engineering. Its platform lets manufacturers and suppliers assess the cybersecurity risks of their products during development and track them across the entire product lifecycle. CYMETRIS combines two perspectives in a single model: a systematic analysis of which attacks a product permits, and continuous visibility into newly discovered vulnerabilities. Architectural changes and emerging threats feed directly into the assessment, allowing manufacturers to justify the proportionality of their security measures and to generate audit-ready evidence for the EU Cyber Resilience Act, UN R155, and ISO/SAE 21434. Built on a reputation earned across the automotive value chain, from OEMs to Tier-N suppliers, CYMETRIS is extending that expertise into further regulated industries. For more information, visit cymetris.com.

About VicOne

VicOne, headquartered in Tokyo, Japan, is a cybersecurity leader for Physical AI, built on proven automotive cybersecurity expertise. Its software and services protect the digital systems that shape how vehicles and robots see, decide, and act. VicOne helps OEMs, Tier 1 suppliers, robot makers, and operators identify cyber risks early, assess their potential safety impact, and protect systems in operation, helping maintain safe, reliable behavior across real-world deployments. With 180+ zero-days uncovered across automotive and robotics, 100M+ new threat intelligence signals added monthly, and 30 U.S. patent applications pending in AIDV and AI security, VicOne combines specialized Physical AI security research with global threat intelligence. As a Trend Micro subsidiary, VicOne is backed by decades of global cybersecurity expertise. For more information, visit vicone.com.

Ling Cheng

VicOne

344002265 ext.

[email us here](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/942964295>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2026 Newsmatics Inc. All Right Reserved.