

IdoubleS presents the Governed Cyber Threat Model at it-sa 2026. AI-generated threat knowledge, validated before the SOC acts on it

In a workshop with CrowdStrike, SVA, and a reference customer from the German defence sector on 27 October, the German cyber security startup will show how threat intelligence becomes a reliable threat model that the customer owns.

NIDDERAU, Germany, 22 October 2026 – IdoubleS Cybersecurity GmbH will present its [Cyber Threat Modelling Platform](#) at [it-sa Expo&Congress 2026](#) (27–29 October, Nuremberg). The platform transforms threat intelligence reports written in natural language into a Governed Cyber Threat Model that shows which adversaries would target which critical business functions and how. From this model, the platform derives native detection rules for SIEM and EDR, guides for threat hunting and incident response, and evidence for [DORA](#), [NIS2](#), and [TIBER-EU](#).

Speed and volume are no longer the question in the Security Operations Centre (SOC). Trust is. AI-based extraction is replacing the manual reading of threat intelligence reports, yet the knowledge it generates often lacks evidence, reliability, confidence levels, and validation. Unverified claims travel as fast as verified ones, and the verified and the merely plausible look alike. IdoubleS answers this with Trust by Design, every claim in the model carries evidence, confidence and validation, and an analyst approves it before a rule, a hunting hypothesis or an AI agent acts on it.

At it-sa, IdoubleS will demonstrate the platform live. On 27 October, in the workshop “[Intelligence-Driven Cyber Threat Modelling – From CTI to Real-World Defence](#)” (Room Lissabon, Level 1, NCC Mitte), the company will show, together with the project partners [CrowdStrike](#) and [SVA](#), how the model is built and how it was validated with a reference customer from the German defence sector. The morning session is aimed at decision-makers and summarises the results of the reference project; the afternoon session is aimed at a technical audience. Programme and registration: idoubles.net/en/events/series/it-sa-2026-ctm

IdoubleS is a German start-up, privately financed with German capital. To comply with digital sovereignty requirements, the platform is built on open-source frameworks, runs in the cloud, on-premises or in air-gapped environments, comes with built-in AI models, and exports the threat model in the open [STIX 2.1](#) standard. Knowledge of an organisation’s own threat landscape stays with the customer, vendor-agnostic, and auditable.

“The question is no longer how fast an AI model reads a threat intelligence report, but whether you can trust the result before you act on it. That is what we will show at it-sa, with our project partners and a customer who has validated it with us,” says Rukhsar Khan, *founder and CEO of IdoubleS Cybersecurity GmbH*.

About IdoubleS Cybersecurity GmbH

IdoubleS Cybersecurity GmbH, based in Nidderau, Germany, is an independent, privately financed cybersecurity company combining deep R&D with specialised cybersecurity services and proprietary technology. Its IdoubleS Cyber Threat Modelling platform transforms threat intelligence into governed, evidence-backed and validated cyber threat models, leveraged for SOC and cybercrime use cases. The company serves customers in Germany, the DACH region, and the wider EU, building on open-source frameworks to promote technological sovereignty and vendor independence.

[Governed Cyber Threat Model – Trust by Design.](#)

© 2026 IdoubleS Cybersecurity GmbH. All rights reserved.

– Ends –

Press contact

Aisha Khan
IdoubleS Cybersecurity GmbH
Email: press@idoubles.net
Phone: +49 6187 2004572

For more information, please visit: www.idoubles.net