

IdoubleS stellt auf der it-sa 2026 das Governed Cyber Threat Model vor. KI-generierte Threat-Knowledge – validiert, bevor das SOC darauf basierend handelt

In einem Workshop mit CrowdStrike, SVA und einem Referenzkunden aus dem deutschen Verteidigungssektor am 27. Oktober zeigt das deutsche Cybersecurity-Startup, wie aus Threat-Intelligence ein verlässliches, kundeneigenes Cyber-Threat-Model entsteht.

NIDDERAU, Deutschland, 22. Oktober 2026 – Die IdoubleS Cybersecurity GmbH präsentiert auf der [it-sa Expo&Congress 2026](#) (27.-29. Oktober, Nürnberg) ihre neue [Cyber Threat Modelling Plattform](#). Die Plattform überführt Threat-Intelligence-Reports in natürlicher Sprache in ein Governed Cyber Threat Model, das aufzeigt, welche Angreifer welche kritischen Geschäftsfunktionen auf welche Weise bedrohen würden. Aus diesem Modell leitet die Plattform native Detektionsregeln für SIEM und EDR, Leitfäden für Threat Hunting und Incident Response sowie Nachweise für [DORA](#), [NIS-2](#) und [TIBER-EU](#) ab.

Tempo und Volumen sind im Security Operations Center (SOC) nicht mehr die entscheidende Frage. Entscheidend ist Vertrauen. KI-gestützte Extraktion ersetzt zunehmend das manuelle Lesen von Threat-Intelligence-Reports, doch dem so gewonnenen Wissen fehlen häufig Belege, Zuverlässigkeit, Konfidenzangaben und Validierung. Ungeprüfte Aussagen verbreiten sich so schnell wie geprüfte, und verifizierte Aussagen sind von lediglich plausiblen kaum zu unterscheiden. IdoubleS begegnet dieser Herausforderung mit Trust by Design: Jede Aussage im Modell ist mit Belegen, einer Konfidenzangabe und einem Validierungsstatus versehen. Ein Analyst gibt sie frei, bevor eine Detektionsregel, eine Hunting-Hypothese oder ein KI-Agent auf ihrer Grundlage handelt.

Auf der it-sa demonstriert IdoubleS die Plattform live: Am 27. Oktober zeigt das Unternehmen im Workshop „Intelligence-Driven Cyber Threat Modelling – From CTI to Real-World Defence“ (Raum Lissabon, Ebene 1, NCC Mitte) gemeinsam mit den Projektpartnern CrowdStrike und SVA, wie das Modell aufgebaut wird und wie es mit einem Referenzkunden aus dem deutschen Verteidigungssektor validiert wurde. Die Session am Vormittag richtet sich an Entscheidungsträger und fasst die Ergebnisse des Referenzprojekts zusammen. Die Nachmittagssession adressiert das technische Fachpublikum. Agenda und Anmeldung:

<https://idoubles.net/de/events/series/it-sa-2026-ctm>

IdoubleS ist ein deutsches Startup, das privat mit deutschem Kapital finanziert wird. Um Anforderungen an digitale Souveränität zu erfüllen, baut die Plattform auf Open-Source-Frameworks auf, läuft in der Cloud, On-Premises oder in Air-Gapped-Umgebungen, umfasst integrierte KI-Modelle und exportiert das Cyber-Threat-Modell im offenen Standard STIX 2.1. Das Wissen über die eigene Bedrohungslandschaft bleibt beim Kunden, herstellerunabhängig und prüfbar.

„Die Frage ist nicht mehr, wie schnell eine KI einen Threat-Intelligence-Report liest, sondern ob man dem Ergebnis trauen kann, bevor man danach handelt. Genau das zeigen wir auf der it-sa, mit unseren Projektpartnern und einem Kunden, der dies mit uns validiert hat“, sagt Rukhsar Khan, Gründer und CEO der IdoubleS Cybersecurity GmbH.

Über IdoubleS Cybersecurity GmbH

Die IdoubleS Cybersecurity GmbH mit Sitz in Nidderau ist ein unabhängiges, privat finanziertes Cybersecurity-Unternehmen, das tiefgehende F&E mit spezialisierten Cybersecurity-Dienstleistungen und eigener Technologie verbindet. Die IdoubleS Cyber Threat Modelling Plattform überführt Threat Intelligence in governed, evidenzbasierte und validierte Cyber-Threat-Modelle, die für SOC- und Cybercrime-Anwendungsfälle genutzt werden. Das Unternehmen betreut Kunden in Deutschland, der DACH-Region und darüber hinaus in der gesamten EU und setzt auf Open-Source-Frameworks, um technologische Souveränität und Herstellerunabhängigkeit zu fördern.

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

© 2026 IdoubleS Cybersecurity GmbH. Alle Rechte vorbehalten.

– Ende –

Pressekontakt

Aisha Khan
IdoubleS Cybersecurity GmbH
E-Mail: press@idoubles.net
Tel.: +49 6187 2004572

Weitere Informationen unter: www.idoubles.net