THREATGET

Die automatisierte Lösung für die Bedrohungsanalyse vernetzter Systeme

In einer zunehmend digitalisierten Welt, in der Fahrzeuge, Industrieanlagen und kritische Infrastrukturen eng vernetzt sind, wird Cybersecurity zu einem zentralen Faktor für Sicherheit, Zuverlässigkeit und Regulierungskonformität. Gerade im Bereich des Internet of Things (IoT) und bei Cyber-Physischen Systemen steigt die Komplexität rasant – ebenso die Zahl potenzieller Bedrohungen. Traditionelle, rein manuell durchgeführte Gefährdungsanalysen stoßen hier an ihre Grenzen. THREATGET schließt diese Lücke: Die Lösung automatisiert Bedrohungsanalysen, modelliert Risiken früh im Entwicklungsprozess und sorgt dafür, dass Systeme bereits bei ihrer Entstehung „security by design" erfüllen. Mit der kontinuierlich aktualisierten Threat-Datenbank, der Integration in die etablierte Modellierungsplattform Enterprise Architect und dem Fokus auf sicherheitskritische Branchen wie Automotive, Rail, Energie und Transportinfrastruktur bildet THREATGET eine skalierbare und effizient einsetzbare Basis für moderne Cybersecurity-Engineering-Prozesse.

Fakten

- Lösungsbereich: **Organisationen, Prozesse, Qualitätssicherung und Zertifizierung, Technologische Innovation**
- Verwaltungsebene: **Bundesland, Bund**
- Lösungsprozess: **Digitalisierung und Technologie, Mobilität und Transport, Sicherheit und Verteidigung, Wissenschaft und Forschung**
- Technologie: **Informationstechnologie, Internet of Things, Künstliche Intelligenz, Netzwerke, Plattformtechnologie**

So funktioniert es

THREATGET basiert auf einem modellbasierten Engineering-Ansatz, der Cybersecurity früh in die Entwicklung integriert. Systemarchitekturen werden in Enterprise Architect modelliert und automatisch mithilfe eines kuratierten, laufend aktualisierten Threat-Katalogs analysiert, der sicherheitsrelevante Elemente, Angriffsmuster und Schwachstellen abbildet. Vordefinierte Sicherheitsparameter ermöglichen eine konsistente Bewertung. Das Tool identifiziert Risiken, zeigt Angriffsszenarien auf und empfiehlt Gegenmaßnahmen. Alle Risiken bleiben über den gesamten Entwicklungsprozess hinweg nachvollziehbar – inklusive normkonformem Reporting. Hohe Automatisierung macht Analysen reproduzierbar, präzise und aktuell, während unternehmensspezifische Bedrohungen ergänzt werden können. THREATGET unterstützt zudem regulatorische Anforderungen wie ISO/SAE 21434 und UNECE WP.29.

Das große Ganze

THREATGET ermöglicht es Unternehmen, Cybersecurity systematisch von Beginn an zu verankern und Compliance effizient zu erfüllen. Besonders im Automotive-Sektor – geprägt von wachsender Softwarekomplexität und Vernetzung – wird strukturiertes Risikomanagement zum entscheidenden Wettbewerbsfaktor. Hersteller, Zulieferer, Prüfstellen und Infrastrukturbetreiber profitieren von frühzeitiger Risikoerkennung zur Kostensenkung, automatisierten Analysen für schnellere Entwicklungszyklen, standardkonformen Reports zur Unterstützung von Zertifizierungen sowie kontinuierlich aktualisierter Threat Intelligence zur Stärkung der Resilienz. Gleichzeitig zeigt THREATGET die Innovationskraft österreichischer Forschung und Industrie. Die „made in Austria"-Lösung wurde mit dem Constantinus Award ausgezeichnet, setzt internationale Maßstäbe und wird zunehmend auch in weiteren Branchen mit sicherheitskritischer Infrastruktur eingesetzt.