THREATGET

The Automated Threat Analysis Solution for Networked Systems

In an increasingly digital world, where vehicles, industrial plants and critical infrastructures are highly interconnected, cybersecurity has become a key factor in safety, reliability and regulatory compliance. Particularly in the Internet of Things (IoT) and cyber-physical systems, complexity is rising sharply – and so is the number of potential threats. Traditional, purely manual threat assessments are no longer sufficient. THREATGET closes this gap: the solution automates threat analysis, models risks early in the development process and ensures that systems meet "security by design" principles from the outset. With its continuously updated threat database, its integration into the well-established Enterprise Architect modelling platform, and its focus on safety-critical sectors such as automotive, rail, energy and transport infrastructure, THREATGET provides a scalable and efficient foundation for modern cybersecurity engineering.

How it works

THREATGET is based on a model-based engineering approach: at an early stage of system development, system architectures are modelled in the Enterprise Architect environment and automatically analysed for security risks. The tool uses a domain-curated, continuously updated threat catalogue that systematically maps security-relevant elements, attack patterns and potential vulnerabilities. All model elements contain predefined security parameters, enabling a formally consistent evaluation. Based on these modelled structures, the tool identifies potential security issues, highlights specific attack scenarios and proposes appropriate mitigations. All identified risks remain traceable throughout development and qualification, including standard-compliant reporting. Its high degree of automation makes security analyses repeatable, less error-prone and always up to date. The option to add organisation-specific threats or model elements further expands its applicability across a wide range of safety-critical domains. With regard to modern regulatory requirements – such as ISO/SAE 21434 or UNECE WP.29 – THREATGET enables fully documented, compliant cybersecurity engineering.

The Big Picture

THREATGET addresses a core need of modern industries: the ability to systematically integrate cybersecurity into development from the very beginning while meeting compliance requirements efficiently. Especially in the automotive sector, where vehicles today contain millions of lines of code and continuously communicate with infrastructure, backend systems and sensor networks, risk management has become a decisive competitive factor. Manufacturers, suppliers, technical inspection bodies and infrastructure operators all benefit: early risk detection reduces development and downstream costs; automated analyses accelerate development cycles; standard-compliant reports support certification processes; and continuously updated threat intelligence strengthens long-term system resilience. Moreover, THREATGET demonstrates how Austrian research and industry jointly set international benchmarks: the combination of the AIT's dependability engineering expertise, the Lieber Group's MBSE know-how and the industrial

Quick Facts

- Solution area: **Organisations, Processes, Quality assurance and certification, Technological innovation**
- Administrative level: **State, Federation**
- Solution process: **Digitization and technology, Mobility and transportation, Science and research, Security and defense**
- Technology: **Artificial Intelligence, Information technology, Internet of Things, Networks, Platform technology**

requirements of the automotive sector has produced a solution that significantly shapes the cybersecurity landscape of European mobility and critical infrastructure.