Cybersecurity at Soloplan: How we make CarLo safe

In an increasingly networked logistics world, cybersecurity becomes more and more important every day. Transport service providers have to face the challenge of protecting sensitive data, securing stable processes and withstand modern forms of attack. As an internationally leading provider of transport management software (TMS), Soloplan highly prioritises this issue–and integrates a high level of security in the software development of **CarLo**, the main solution for efficient transport planning.

The **3SDL model (Soloplan Secure Software Development Lifecycle)** allows Soloplan to make sure that cybersecurity is not only a single process step, but rather a continuous quality feature of all products.

Cybersecurity as a continuous part of our development process

Soloplan banks on an approach on multiple stages which considers security during the entire software lifecycle–from the first concepts to quality assurance. The **continuous level (L0)** plays a key role in it.

Transparent overview of used components

The **Software Composition Analysis (SCA)** allows Soloplan to monitor all used third-party components and libraries for common vulnerabilities. Automated systems check continuously for new CVEs (Common Vulnerabilities and Exposures) in order to detect risks early.

Fast reaction to security alerts

Customers, external partners and employees can report potential security problems. All reports are passed on to the responsible teams, evaluated and fixed in all supported versions–according to our maintenance policy.

Safety awareness in the entire company

New and current employees regularly attend to courses and trainings to understand security standards and actively put them into practice. This continuous knowledge transfer is a main component of our security culture.

Safe software starts with the design

Even before one single line of code is written, Soloplan specifies precise **security requirements**. Product managers, customer solution experts, software engineers and quality assurance specialists work together closely to detect risks early.

In **architecture and concept reviews**, possible attack scenarios are analysed already during the concept phase and evaluated in the form of “threat modelling”. This way, potential security risks are proactively eliminated before they emerge.

Security in development: Code, tests and automated analyses

As soon as the development begins, the measures of the **L2 level** apply.

Quality thanks to peer review

Experienced developers verify each code modification before the commit. Findings from the architecture phase as well as our internal coding guidelines are incorporated. Goal: Detect problems before they reach the product.

Targeted tests of security-related areas

Modules such as data integrity, access control or encryption are fully verified via **security unit tests**. These tests make sure that security-critical areas work reliably at any time.

Automated static code analysis

After each commit, a SAST system checks the code for possible vulnerabilities or anti-patterns. This way, errors are detected even before the software is executed in the first place.

Quality assurance thanks to realistic attack scenarios

Before any CarLo versions are released to customers, Soloplan runs intensive tests on the software on **L3 level**.

Dynamic Application Security Testing (DAST)

In a sandbox environment, we simulate attacks on running systems. These black-box tests reveal vulnerabilities that are visible only when running the program.

Documentation and best practices

All security-related hints–for example, concerning the firewall rules, port configurations or network architectures–are documented in a structured way. This way, we make sure that CarLo also runs in a safe environment on the customer's systems.

Professional penetration tests

Regular **pentests** complete the automated processes. In realistic attack scenarios, security experts verify our systems from different perspectives–internally and externally.

The results are included in detailed test reports that prioritise vulnerabilities and contain precise recommendations for action. Every identified vulnerability is consistently fixed before release.

Conclusion: Security is not a feature–it is our standard

Thanks to the 3SDL model, Soloplan makes sure that cybersecurity is an integral part of the product development–from the first idea and coding to the final release.
For CarLo customers, this means:
highest security, **continuous quality** and **trust in a software that is actively protected against modern cyber threats**.

Soloplan is consciously investing in processes, tools and people to ensure that CarLo makes the future of the transport sector not only more efficient, but also safer.

Would you also like to rely on a safe logistics software that is protected against cyber-attacks?

Our experts will be glad to show you how CarLo makes your processes safe.

Secure your free presentation appointment

Learn more about the TMS CarLo