



## Knowledge transfer from research to practice

The Cybersecurity Learning Lab is a network of eight Fraunhofer Institutes and ten universities of applied sciences. As part of the Fraunhofer Academy continuing education programme, it supports companies and public authorities in the targeted development of IT security skills.



Lernlabor  
Cybersicherheit



### Contact

**Vivija Čeprkalo-Simić**  
Project Manager  
Cybersecurity Learning Lab  
Phone: +49 89 3229986-138  
vivija.ceprkalo@aisec.fraunhofer.de

### More Information



Fraunhofer Academy

## Knowledge creates security

Detecting attacks early, remaining capable of acting and quickly returning to normal operations – cyber resilience is essential in light of the increasing number of attacks and legal standards. Those who are unfamiliar with this area risk considerable damage. Fraunhofer AISEC provides support in the Cybersecurity Learning Lab with the latest research findings.

### Checking one's own cyber resilience

The first step towards resilience against cyber threats is to assess your current location:

- Does your company use protective mechanisms for data transmission and storage?
- Is your network continuously monitored for attacks?
- Are there contingency plans in place to maintain business operations in the event of an emergency?
- Are regular backups performed?

The online questionnaire from the Cybersecurity Learning Lab provides organisations with initial feedback on where they stand in terms of cyber resilience. Specific action requirements are developed in a personal workshop tailored to the industry, business model and regulatory framework. There is no one-size-fits-all solution: while critical infrastructure facilities such as power suppliers must remain operational despite a cyber-attack, the focus for automotive suppliers is on quickly restoring normal operations after an attack.

### Direct access to application-oriented research knowledge

Depending on individual needs, Fraunhofer AISEC trainers provide targeted training in the Cybersecurity Learning Lab to develop the skills that the organisation requires. Whether for product owners, software developers or IT security officers, in-house

training programmes are customised to fit into everyday work routines and enable participants to implement measures immediately.

### From science to practice

Two practical examples show how scientists pass on their expertise:

- **Dr. Nicolas Müller** explains how machine learning models can be made more resilient to attacks, manipulation, and data leaks. With this knowledge, banks, and payment service providers, for example, can secure their AI models so that suspicious transactions are reliably detected – without fraudsters being able to outsmart the system.

- **Albert Stark** demonstrates methods for designing embedded systems in such a way that even in the event of an attack, basic functions, e.g. in industrial plants, continue to run. Such minimal operation is crucial, for example, in wind turbines, oil refineries or blast furnaces, where it is difficult or expensive to shut down operations.

'The advantage of our training programmes is the comprehensible and practical presentation of highly specialised topics,' explains Vivija Čeprkalo-Simić, project manager of the Cybersecurity Learning Lab at Fraunhofer AISEC. 'Companies come to us specifically for advanced machine learning or post-quantum cryptography because training at this level of depth is not available anywhere else.' Those who invest strategically in this expertise not only protect their systems and data, but also equip themselves for new challenges.