TÜV SÜD CyberSecurity Certified (CSC) Certification

Consumer Internet of Things (CIoT) systems have gained importance in recent years. Securing these systems is paramount for consumers and users.

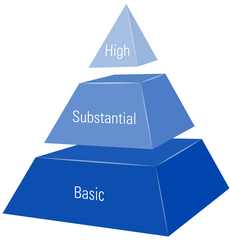
TÜV SÜD CYBERSECURITY CERTIFIED (CSC) CERTIFICATION

- Real certification with mark, independent of manufacturer.
- Based on the GS (Geprüfte Sicherheit) scheme.
- Continuous quality optimization via knowledge sharing between TÜV organizations.

It aims to:

- Uncover problem areas and security gaps.
- Provide effective remedies.
- Pre-empt issues such as financial loss and damage to company reputation.

3 LEVELS OF TESTING



There are three test levels under the TÜV SÜD CyberSecurity Certified (CSC) Certification.

The scope and depth increase with each level.

The scope of testing includes:

- The IoT system itself
- The manufacturer's security-related processes

FEATURES OF CSC TESTING BY LEVELS

BASIC	SUBSTANTIAL	HIGH
Makes cyber-attacks more difficult and challenging	Provides substantial resistance against cyber-attacks	Provides high resistance against cyber-attacks
Product: Document review and technical testing, including safety	**Product:** Document review and technical testing, including safety	**Product:** Document review and technical testing, including safety
Company: Testing of internal processes	**Company:** Testing of internal processes	**Company:** Testing of internal processes
	Penetration test	Cloud test
	Cloud test	Inclusion of suppliers/ subcontractors
	Inclusion of suppliers/ subcontractors	All ETSI EN 303 645 mandatory requirements and additional tests
	All ETSI EN 303 645 mandatory requirements and additional tests	TÜV SÜD penetration test (including source code review) and additional tests

HOW CAN THE TÜV SÜD CSC CERTIFICATION HELP?

1. IMPROVEMENT OF CYBERSECURITY

- Streamlines processes.
- Raises manufacturer awareness of cybersecurity.
- Identifies vulnerabilities and weaknesses.

2. PROVISION OF CIOT MARK

- Ensures that standards are met and comply with emerging regulations around CIoT devices.
- Attests manufacturer readiness in responding to potential security issues.

3. HOLISTIC SUPPORT

- Enables access to a global network of test facilities and cybersecurity experts.
- Provides comprehensive service offerings.
- Includes entire IoT ecosystem (app and cloud) under scope.
- Supports manufacturer for entire product lifecycle.

Find out more about TÜV SÜD's cybersecurity solutions.
www.tuvsud.com/cybersecurity