Choose certainty.
Add value.

Penetration testing

Safeguard your Industrial IT Systems and Critical Infrastructures against Vulnerabilities.

Your challenges

Industrial Control Systems (ICS) components are used for many purposes. They are required to run on different operating systems and be available with a variety of interfaces. This complex and heterogeneous environment means that ICS have a broad attack surface and are vulnerable to malicious attacks from outside parties that can impact the overall functional safety of the entire system. To prevent attacks, companies should identify the vulnerabilities within their system and understand how attackers work.

What is penetration testing?

Penetration testing approaches ICS components from the potential attacker's point of view. TÜV SÜD penetration tests use the same methods as attackers. This involves making an active analysis of the system for potential vulnerabilities arising from system configuration. Our experts also seek out known and unknown flaws in software and in technical countermeasures. In our Industrial IT Security laboratory, we further simulate environments typical for production plants. This enables us to extend penetration tests to essential IT infrastructure used in production environments and critical infrastructures.

Why is penetration testing important for your business?

By helping you understand your system's vulnerability to external threats, penetration testing enables you to prevent malicious attacks. The penetration test serves as a benchmark for the actual security level of your industrial IT product. Following testing, you receive a prioritised list of security measures that are critical to safeguard your system. Implementing these measures helps to protect your business from reputational damage and the financial cost of recouping lost information.

FOUR STEPS FOR BETTER INDUSTRIAL IT SECURITY

Handover the device to be tested.
Develop a test environment.
Handover relevant documents, if any.

Catalogue information available to the public.
Scan services, patch level, operating system, etc.
Robustness testing.

Attempt to gain access based on vulnerabilities.
Circumvent access rights (privilege escalation)
Compromise data.

Describe and evaluate the identified security holes.
Compile and review the test report including a management summary.

Our penetration testing services

TÜV SÜD provides the following penetration testing services.

- **Robustness testing**
  Our experts utilise the latest tools to execute robustness testing on the device under test (DUT). We test the effects of high load on the network interfaces of the DUT, as well as malformed packets (fuzzing). Supported protocols include LLDP, ARP, Ethernet, ICMP, IGMP, IP, TCP, UDP, DNP3, Ethernet/IP, MMS, Modbus/TCP, OPC UA, FTP, HTTP, NTP, RDP, RPC, SNMP, telnet and ZigBee.
- **Penetration testing**
  Based on the results of robustness testing and other information gathering techniques, our experts conduct attacks on the DUT. These attacks include manually developed exploits for unknown vulnerabilities.
- **Penetration testing report**
  Following penetration testing, we provide you with a report describing all the identified vulnerabilities, including an assessment of the severity of these weaknesses.

Your business benefits

- **Save money** – with a prioritised list of measures that enables you to focus your resources on overcoming the identified vulnerabilities.
- **Save time** – by leveraging our expertise and tools to swiftly identify vulnerabilities and bring your product to market sooner.
- **Improve product quality** – by identifying and rectifying essential security vulnerabilities during the penetration test process.
- **Minimise risk** – by ensuring that your products and systems are protected against malicious attacks that can result in loss of reputation and money.

Why choose TÜV SÜD?

TÜV SÜD offers a holistic approach to safety and security. Our long-term experience of industrial environments combined with our expertise in industrial IT security and process knowledge ensures we possess the qualifications and capabilities to carry out an in-depth assessment of your IT security. As a one-stop solutions provider, our experts offer guidance and comprehensive services throughout the value chain. We work closely with many industry partners on various topics such as renewable energy, industrial IT security and functional safety. Our experts also actively participate in international standardisation committees. This enables us to serve you with valuable insights for product development.

Choose certainty. Add value.

TÜV SÜD is a premium quality, safety and sustainability solutions provider that specialises in testing, inspection, auditing, certification, training and knowledge services. Represented in over 800 locations worldwide, we hold accreditations in Europe, the Americas, the Middle East, Asia and Africa. By delivering objective solutions to our customers, we add tangible value to businesses, consumers and the environment.

Related services

TÜV SÜD provides the following related services:

- Industrial IT Security – Risk Analysis
- Industrial IT Security – Security Check
- System and device certifications based on IEC 62443
- Inspection to Rail standard DIN VDE V 0831-102