REST ASSURED.

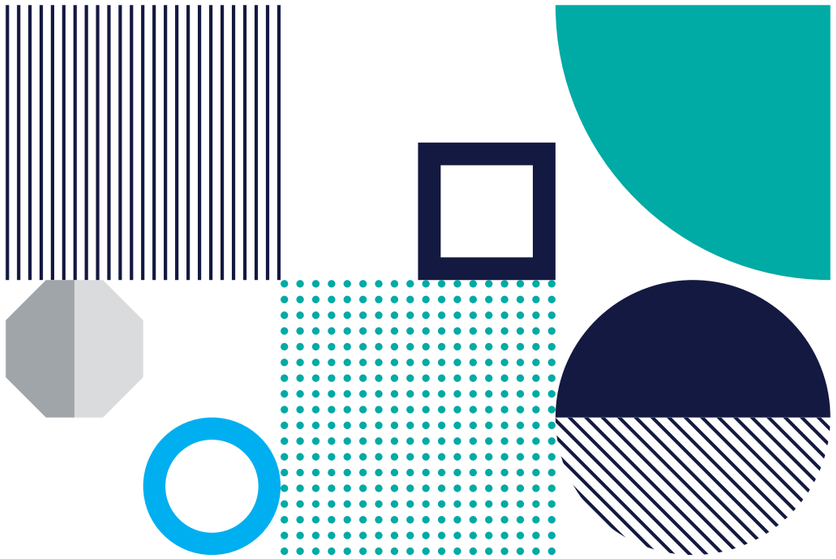
Penetration test

PINPOINT CYBER SECURITY WEAK POINTS

www.csis.dk

Why should you conduct a penetration test?

- Improve your security posture
- Determine whether your critical assets and data are actually at risk
- Avoid financial, operational and reputational losses caused by cyber attacks
- Identify cyber security weaknesses before an attacker exploits them
- Get quantitative results that help measure the risk associated with your critical assets
- Gain insight into attacker motivations and most likely targets



A single vulnerability can act as an open door to criminals.

Malicious actors determined to gain control of your business will find it.

Discover how vulnerable your most critical assets are to cyber attacks.

How it works

CSIS supplies a laptop to the customer, who then connects the laptop to the organisation's network. The laptop establishes a secure VPN connection back to CSIS, either via the organisation's network, or via a built-in 3G mobile connection.

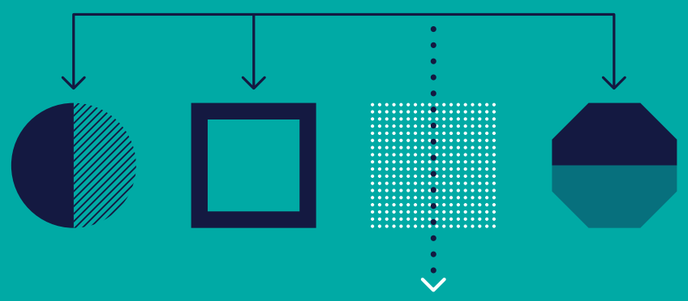
The laptop observes, collects and analyses information flowing through the organisation's network. The work is primarily manual, although some processes are automated.

The test will typically run for 2-4 weeks, although this figure varies according to the nature of the organisation and IT setup.

As results accumulate during this period, CSIS increases the amount of active testing and applies a range of simulated attacks. The actual man hours spent on this are typically much less than the total duration of the test.

The customer may set up 3 pre-defined targets for simulated attack (e.g. customer data on a single drive, the organisation's ERP system, or even accessing the CTO's email).

CSIS penetration test



Active testing and simulated attacks are aimed at uncovering even the most obscure network vulnerabilities.

CSIS Penetration test

IMPROVE YOUR CYBER SECURITY POSTURE

Penetration tests may include, but are not limited to

- Scanning for systems that are not updated
- Exposing insufficient network protection
- Use of weak user credentials
- Exploitation of vulnerabilities in embedded devices
- Try to gain domain admin credentials
- Extraction of data

The risks of not conducting a penetration test

- Financial, operational & reputational loss
- Theft of your intellectual property
- Penalties or damages due to exposed customer data
- Lack of insight into the organisation's level of risk exposure
- Reduced availability of data or systems
- Weakened confidence in the organisation
- Corrupted corporate website content

A CSIS penetration test will improve your security posture by identifying security weaknesses before a real attacker can exploit them.

SCOPE AND DURATION

Standard penetration test

A standard penetration test requires that the laptop has a continuous supply of power and continuous access to the customer network for the entire duration of the test. A standard penetration test is carried out over a 2-4 week period.

A technical report usually takes 1-2 days to create, but may take a day longer if the number of vulnerabilities found are excessive, or if a management summary is required.

OVERVIEW

Automated and manual testing

CSIS's penetration tests are based on a user who has no rights in the organisation's systems, simulating the tools, tactics and procedures of a real-world attacker's breach of the organisation's internal network.

CSIS penetration tests are a combination of automated and manual testing, and all results are verified manually to eliminate false positives from the report.

Additional service options

If the customer wants to test an initial attack vector (e.g. phishing, spear-phishing, tailgating, burglary, lost USBs) this can be done by extending the scope before work starts.

CSIS
Penetration test

DELIVERABLES

What you get

- High level executive summary (PowerPoint in either Danish or English).
- A technical section (in English), including weighted risk levels and general observations.

Additional options

- An extended management summary document.
- Risks and consequences.
- Proof of concept.

Learn more

For more information, please contact us at **www.csis.dk**

REST ASSURED.

CSIS IN BRIEF

- Employee-owned Group founded in Copenhagen in 2003.
- IT security provider to some of the world's largest financial services and enterprise organisations.
- Credited by Gartner Group for outstanding threat intelligence capabilities.
- Renowned for penetration testing, incident response, forensics and malware reverse engineering capabilities.

CSIS Security Group A/S

Head office
Vestergade 2A, 3rd floor
1456 Copenhagen,
Denmark

+45 88 13 60 30
contact@csis.dk

www.csis.dk