Cyber Security Advisory Services

Find out if your business is prepared to withstand modern-day cyber attacks

Why businesses need a security assessment

As businesses jump on the digital bandwagon and implement digital initiatives, the total attack surface increases. Besides this, methods of cyber attacks are growing sophisticated, and the number of new threats is also increasing. With so many variables, it is important for businesses to have a strong security posture.

A weak security posture can lead to:

- financial losses due to ransom
- high costs due to downtime
- loss of business data and information
- loss of customer trust and reputation
- legal and compliance hurdles

Average cost of data breach: US$ **4.35 M**

Average costs saved with advanced security: US$ **3.05 M**

* Source: https://www.ibm.com/in-en/reports/data-breach

To defend against modern attacks, businesses first need to understand whether they have the right security architecture. Hence, they must analyze their architecture and identify the gaps – which is why they need to take security assessments.

Security assessments involve the evaluation of numerous processes like network scanning, penetration testing, vulnerability assessment, threat modelling, cloud security, Operation Technology (OT) analysis, and more.

Different assessments serve varied purposes. For instance, a vulnerability assessment will check for loopholes in your settings, configuration, setup, etc. whereas a penetration assessment will simulate an attack on your system to check the response of your defense.

What to expect from security assessment

An organization with a small in-house security team and limited tools will have a hard time coping with ever-increasing cyber risks. Therefore, it may not assess its own security levels.

With security assessments, here's what we can determine:

- The risk to your systems and business
- How well the current security solution is operating
- The gaps in the current security architecture
- How to reduce these gaps
- How to make effective security investments
- Ways to measure security performance
- A roadmap to achieve higher security maturity levels

To give you an idea of the assessment process, here are some standard steps:

1 Initial engagement: agenda-setting

2 Architecture review: stakeholder (architects, operational team, C-level, GRC team) interviews and workshop

3 Assessments: running surveys and assessments

4 Analysis: identifying the correlation between threats, assets, and vulnerabilities

5 Publication: report is published with the results

6 Delivery: customized recommendations and roadmap based on the results

T Systems

Let's power higher performance

Magenta security expertise

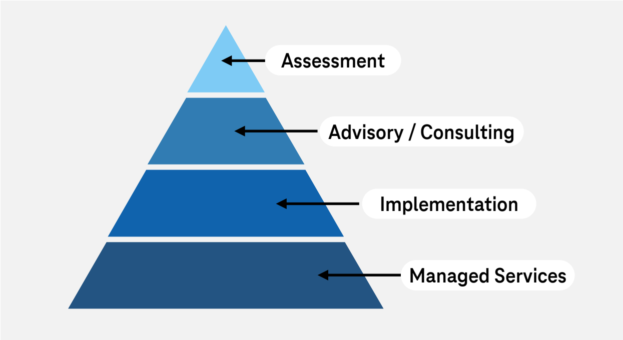
If you've any questions about security assessments or need advisors to look at your security architecture, we can help you.

We can support you with:

- Assessing current IT architecture
- Assessing OT architecture
- Assessing SASE architecture
- Assessing zero trust architecture
- Cloud & network configuration
- Penetration Testing
- CISO-as-a-Service and more.

We can support you to pick the right cyber security solution that matches your business needs.

Together, we create a roadmap to enhance your security maturity levels. This way, you not only protect data and applications, but also move towards secure digital transformation with a strategic security advantage.



Your cyber security in safe hands:

- Pool of experienced security advisors
- Latest tools and platforms for assessments
- One of the largest Security Operations Centers (SOC)
- 200+ cyber security experts in the SOC alone
- Rich partner ecosystem & best solutions for implementation
- Proven experience in Managed Services

Expert Contact

Andreas Pecka
Head of International Expert Sales &
Presales Cyber Security
a.pecka@t-systems.com

Published by

T-Systems International GmbH
Hahnstraße 43d, 60528 Frankfurt am Main, Germany
Email: cyber.security@t-systems.com
Internet: www.t-systems.com

Last update: 10/2023

T Systems

Let's power
higher performance