










Kaspersky Tabletop Exercise

Kaspersky Tabletop Exercise (TTX)

Kaspersky Cybersecurity Services:

-  Kaspersky Tabletop Exercise
-  Kaspersky Managed Detection and Response
-  Kaspersky Cybersecurity Training
-  Kaspersky Incident Response
-  Kaspersky Targeted Attack Discovery
-  Kaspersky Security Assessment
-  Kaspersky SOC Consulting

According to IDC research, only 18% of companies have developed an incident response playbooks.

Test your Incident Response capabilities and improve your cyber resilience

Do you want to improve your cyber resilience and prepare your team to handle new types of cyberattack?

If the answer is 'yes', you need **a security incident response plan** to respond promptly to attacks and limit any damage. Even after you've developed your incident response plan, the job isn't done – it's essential that you keep it up to date and test it regularly against realistic scenarios.

Kaspersky's Tabletop Exercise (TTX) will help you enhance your incident response processes and improve collaboration between teams.

What is Kaspersky Tabletop Exercise?

Kaspersky TTX is a guided exercise that validates an organization's incident response procedures and plans. It identifies gaps in the incident response process, clarifies different roles and responsibilities across teams, and improves coordination between departments during an incident.

Kaspersky's Global Emergency and Response Team (GERT) creates a tailored incident scenario which reflects the current threat landscape and the customer's operational needs. The real-life incident scenarios as possible and are based on GERT's extensive experience in investigating complex attacks for organizations in different industries across the world.

Kaspersky TTX involves:



Lively interactions and discussions based on real incidents



An open environment where participants gain practical knowledge while having fun



Tailored to the audience: security specialists, executive team, or both

Key results/benefits:

Your team will be able to test exactly how ready they are to handle real incident response incidents

Executives, information security specialists, and managers from other departments will all gain a better understanding of their roles and responsibilities in the incident response process

Coordination and cooperation between departments will be improved



How the service works

The Kaspersky TTX can be conducted onsite or remotely.

1

Onboarding

Workshop to:

- Establish what the company's response process looks like
- Understand the operational environment
- Identify any specific areas of concern
- Get a sense of the current threat landscape

2

Design

Kaspersky experts develop a scenario with injects tailored to the customer's overall incident response plan based on their environment and infrastructure, and taking into account their concerns and objectives

3

Role play

All the participants are briefed with their roles and an attack scenario. Kaspersky experts evaluate the team's actions and decisions and check if they align with the incident response plan

4

Lessons learned

The report includes:

- The report includes:
- A rundown of all the steps in the TTX scenario that was used
- A comparison between the expected response and the actual response
- Expert recommendations

Some of the widespread attack scenarios used in Kaspersky TTX include ransomware, phishing, supply chain attacks and insider threats.

During the first stage, Kaspersky security experts conduct an onboarding workshop (onsite or remotely) to get an understanding of the customer's threat landscape, their objectives and any other organizational and technical aspects relevant to design the tabletop exercise.

A project plan is then developed, incorporating regular update meetings, TTX execution and a final report plus interviews with different stakeholders (optional) in order to design and create a **tailored scenario** that will put your incident response plan to the test before it becomes a reality.

During an information security incident, different stakeholders are involved, and the same goes for the Tabletop Exercise. Mean testing incident response capabilities takes into account technical specialists as well as, for instance, members of the cyber crisis management team.

After the exercise, a report is provided, which includes a rundown of all the steps in the TTX scenario that was used, information on the injects, identified gaps based on a comparison between the actual response and the expected response based on best practices.

About Kaspersky GERT



The Kaspersky Tabletop Exercise service is delivered by our Global Emergency and Response Team (GERT), leveraging its vast practical experience and expertise in incident response best practices.



GERT is a group of global experts that has been investigating complex information security incidents for organizations in different industries and regions for more than 10 years. GERT experts are certified in Information Security Incident Management, Digital Forensics, Malware Analysis, Network Security and Risk Assessment.



Kaspersky Tabletop Exercise

[Learn more](#)

www.kaspersky.com

© 2022 AO Kaspersky Lab.
Registered trademarks and service marks
are the property of their respective owners.