

Test and strengthen your incident response readiness

Kaspersky Tabletop Exercise

kaspersky cybersecurity true to business

Kaspersky Tabletop Exercise (TTX)

Are you confident your team can respond effectively to a real cyber incident?

An incident response plan is essential. But without regular testing under real-life conditions, you can't be sure it will perform when it matters most. Cyberthreats evolve rapidly, and your ability to respond must keep pace.

Kaspersky Tabletop Exercise (TTX) helps you validate your incident response capabilities, identify gaps, strengthen cyber resilience, and build the confidence your team needs to act decisively under pressure.

What to expect from Kaspersky TTX

Tailored incident scenarios aligned to your industry, threat landscape and risks

Interactive discussions based on real-world cyberattacks and breach cases

A practical, engaging, hands-on experience

Flexible formats for technical teams, executives or cross-functional groups

Expert-led sessions delivered by Kaspersky's Global Emergency Response Team (GERT)

Real-life incident scenario and injects

Kaspersky's GERT presents the scenario to the players

All working together to respond to the incident

- Executive board
- Cyber crisis management
- Incident Response team
- Blue team
- SOC team
- IT team

How it works

The exercise can be delivered onsite or remotely, depending on your requirements.

Onboarding and preparation

A 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.

At the initial stage, Kaspersky experts conduct a briefing session to assess the customer's current threat landscape, better understand their goals and needs, and identify any organizational and technical factors that may be relevant for the exercise.

Scenario development

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

Project plan development, including regular meetings, exercise schedule, final report and optional participant surveys. All these steps are aimed at creating a tailored scenario that allows you to evaluate the effectiveness of your incident response strategy before a real threat occurs.

Exercise execution

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

Responding to a real incident typically involves multiple specialists, and this is fully reflected in our training. The exercise evaluates not only technical teams, but also other stakeholders, such as members of the cyber crisis management team, ensuring a comprehensive assessment of your organization's incident response capabilities.

Reporting and recommendations

The report includes:

- A rundown of all the steps in the TTX scenario
- A comparison between the expected response and the actual response
- Expert recommendations.

After the exercise, we provide a report that includes a step-by-step analysis of the team's actions during the simulated scenario, details on the injected threats, and identified security gaps based on a comparison of actual performance against incident response best practices.

Delivers real value to your organization

Reduces incident impact

Minimize financial, reputational and operational damage by being better prepared.

Strengthens executive clarity

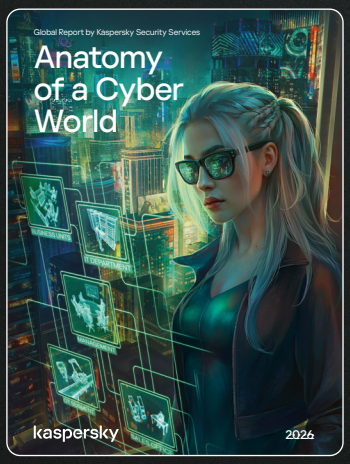
Provide leadership with a clear view of cyber risks and your organization's readiness to detect and respond.

Improves ROI on security investments

Ensure your existing solution, processes and team work together effectively to maximize value and performance.

Train for real-world response

Cyber incidents don't just impact IT – they require coordinated actions across technical teams, leadership and business stakeholders. Kaspersky TTX ensures your people are aligned, prepared and able to make effective decisions under pressure.



Explore our new Security Services Report

Get the report

About Kaspersky GERT

GERT (Global Emergency and Response Team) is a group of global experts that has been investigating complex information security incidents for organizations in different industries and regions for more than 15 years. GERT experts are certified in Information Security Incident Management, Digital Forensics, Malware Analysis, Network Security and Risk Assessment.

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

Kaspersky Tabletop Exercise

Contact us

Powered by Security Services

www.kaspersky.com

© 2026 AO Kaspersky Lab.
Registered trademarks and service marks are the property of their respective owners.

#kaspersky
#truetobusiness