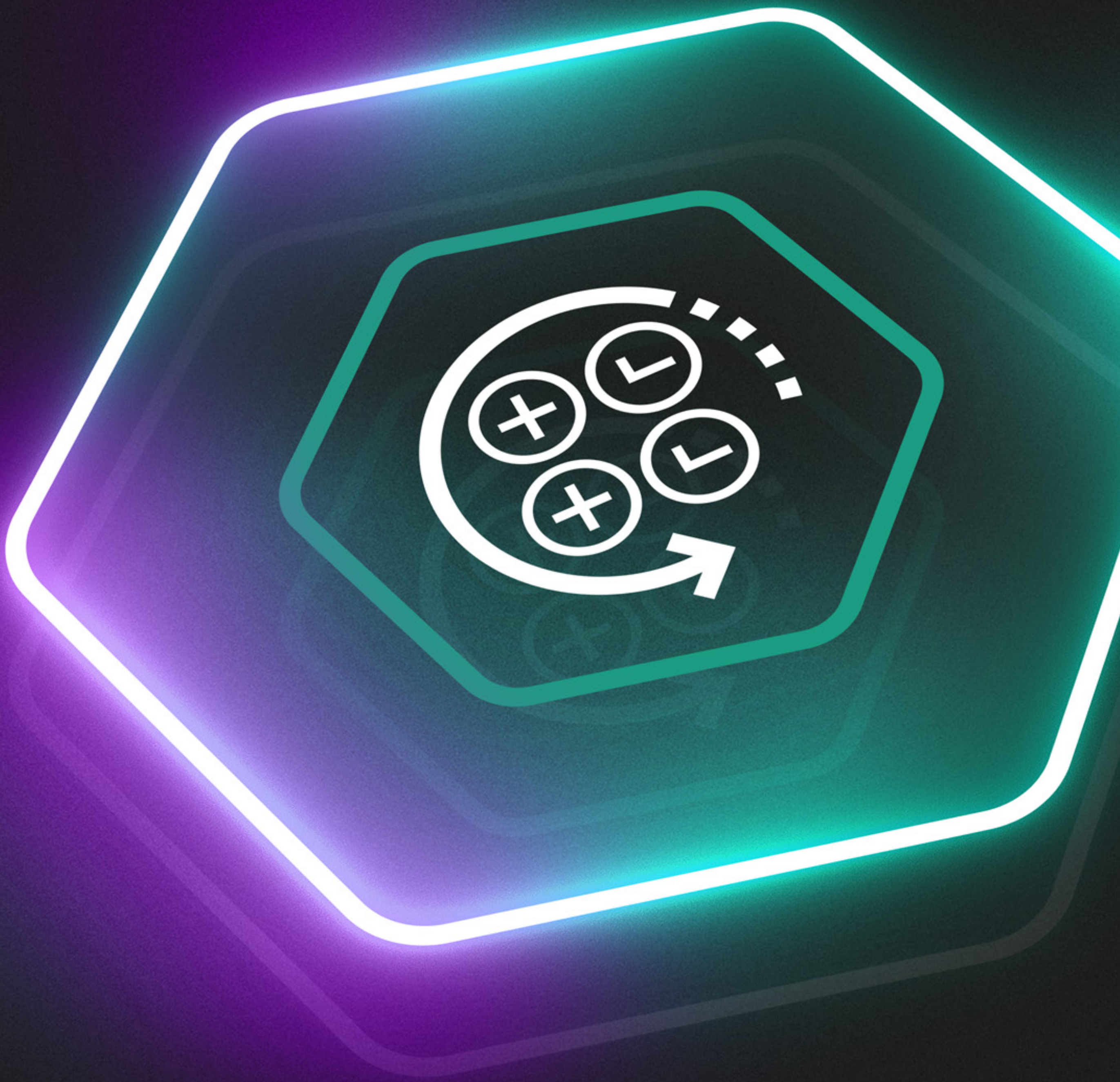

Kaspersky Adversary Attack Emulation

Verifying your SOC's detection capabilities against multiple attack techniques

kaspersky BRING ON THE FUTURE

Find out exactly where you stand

Kaspersky Adversary Attack Emulation provides a detailed assessment of your threat detection capabilities by emulating techniques used by different threat actors at all stages of an attack.

Is your SOC fully equipped to identify sophisticated threats while actively under attack?

Increasingly challenging forms of cyberattack are being launched every day all over the world. But you can only truly gauge your own cyber-detection capabilities in the face of a live attack through a simulation such as Red Teaming or – the worst case scenario – as an incident is actually taking place.

Red Teaming will help assess your team's ability to handle different aspects of a genuine stealth attack - which is great. But most organizations would hesitate to put themselves through such an elaborate, time- and resource-consuming exercise on an ongoing basis.

Kaspersky Adversary Attack Emulation provides the opportunity to regularly check how well your security is able to detect a diverse range of advanced threats, including emerging malware and widespread ransomware, at every stage - with your SOC team's full knowledge and without the resource commitment required for Red Teaming.

You'll be able to:

- Identify gaps in your SOC detection capabilities
- Assess your detection capabilities while actively under attack
- Further refine your SOC team assessment and progress tracking processes
- Train your SOC analysts to work with specific threats/scenarios
- Verify your detection capabilities for specific APT groups
- Build a map of your detection coverage

Kaspersky Adversary Attack Emulation highlights

Specific set of scenarios

Emulation scenarios used are aligned with MITRE ATT&CK and can be customized to your goals, assessing your detection capabilities against specific attack tactics, for example.

Complex evaluation

A granular evaluation process generates multiple scores for different aspects of each detect, giving you a detailed picture of the strengths and weaknesses of your detection capabilities.

Regular basis

The service can be delivered on regular basis, to continuously verify your detection capabilities and track improvement progress.

The selection of test scenarios used in your adversary attack emulation exercise can be based on:

- Techniques used by a specific APT group
- A specific MITRE ATT&CK tactic or tactics
- Techniques used by region-specific or industry-specific APT groups
- The most popular techniques utilized by all APT groups according to MITRE ATT&CK.
- The most popular techniques as identified by Kaspersky Managed Detection and Response (MDR), our latest threat intelligence etc.

How Kaspersky Adversary Attack Emulation works

Our Adversary Attack Emulation service covers key stages of the kill chain related to your internal infrastructure. The emulated tests are mapped to Tactics, Techniques and Procedures (TTPs) as defined in the MITRE ATT&CK framework.

The service can be delivered either on-site and remotely via VPN access, as appropriate.

The process

1

Scope definition and preparation

Understanding your issues and environment, defining the most appropriate set of scenarios and deploying the emulation host.

2

Attack emulation

Running the attack emulation scenarios in accordance with the agreed scope.

3

Purple Assessment

Collecting and processing all the information gained surrounding incident alerts, detections and events.

4

Report preparation

Preparing detailed reporting to identify any gaps and offer our expert recommendations.

You'll receive:

An executive report summarizing

- The obtained results.
- Our conclusions on your current detection capabilities.
- Our recommendations for further improvement.

A detailed technical report containing

- Information on each attack scenario and the corresponding techniques under test.
- Evaluation scores for the detection of each technique which, if the exercise is undertaken regularly, can be also used to measure the progress over the time.
- Recommendations for the optimal detection of each technique.

Why Kaspersky

1 The world's largest independent information security company

With a global presence focused on threat intelligence and technology leadership.

2 Certified Threat Hunters

Our team consists of certified experts in areas including Information Security Incident Management, Digital Forensics, Malware Analysis, Network Security and Risk Assessment.

3 Adaptive Tools and Telemetry

Threats are detected using IoCs, TTPs, IoAs, YARA, and Threat Intelligence.
We can easily modify our detection rules, tools, and telemetry to find new types of threats.

4 Actionable Threat Intelligence

As a global threat intelligence provider, we not only have an extensive deny-listing database but a huge database for allow-listing – all helping us identify threats faster.

Kaspersky Expert Security

Kaspersky Adversary Attack Emulation is one of the many services available as part of our comprehensive Expert Security Portfolio.

Informed

Treat Intelligence

- Threat Data Feeds
- Threat Intelligence Platform (CyberTrace)
- Threat Lookup
- Cloud Sandbox
- APT Intelligence Reporting
- Digital Footprint Intelligence
- Industry-Specific Intelligence Reporting (Financial, ICS, Transport)

Training

- Incident Response Training
- Digital Forensics Training
- Malware Analysis and Reverse Engineering Training
- Online YARA Training

Equipped

Extended Detection and Response

Reinforced

Assessment

- Adversary Attack Emulation
- Compromise Assessment (Targeted Attack Discovery)
- Penetration Testing
- Red Teaming
- Application Security Assessment
- Industry-Specific Security Assessment (ICS, Payment Systems, Transportation, IOT)

Incident Response & MDR

- Managed Detection and Response (MDR Expert)
- Incident Response
- Malware Analysis
- Digital Forensics

Kaspersky Adversary Attack Emulation

Learn more

www.kaspersky.com