Kaspersky Incident Response

kaspersky BRING ON THE FUTURE

No one is immune from attacks: no matter how effective your security controls, you too can become a victim.

The importance of incident response

While your infosec team works hard to ensure that every network component is protected, a single vulnerability could open the door to intruders, giving them access to your information systems.

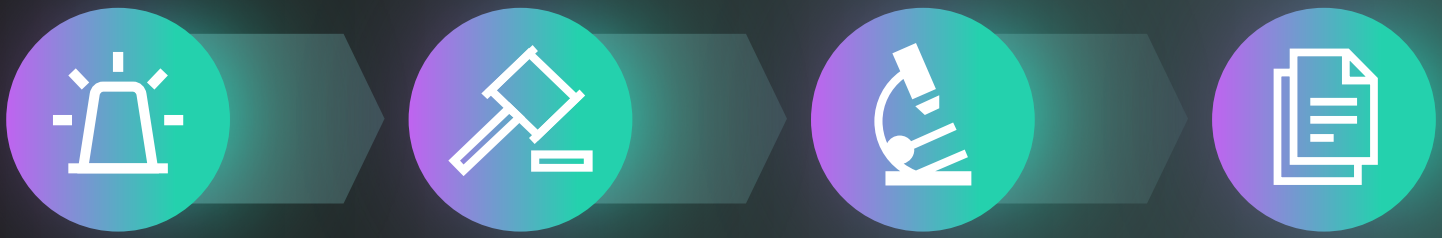
Anything can be targeted. If a system gets hacked, it is vital to establish how it was compromised in order to draw up an attack mitigation plan and prevent such attacks in the future. The incident response service achieves these goals.

Kaspersky Incident Response

How the service works

An incident constitutes a breach or the threat of a breach of computer security policies, acceptable use policies and / or standard security practices.

Incident response — obtains a detailed picture of the incident. The service covers the full incident investigation and response cycle: from early incident response and evidence collection to identifying additional traces of hacking and preparing an attack mitigation plan.



4 stages of incident response

1

Request initialization

At this stage, our experts gather information from those who reported the incident and from IT and other personnel who may have useful knowledge of technical details and business processes to help understand the incident details.

In addition, the Kaspersky team analyzes information about the incident from network and security logs for evidence of the incident. After that, our experts provide short-term recommendations on what to do next.

2

Evidence collection

Depending on the specifics of the incident, the following approaches can be used:

Onsite

Our experts visit your organization and collect evidence related to the incident to aid the investigation

Remote

Our experts provide all necessary tools and guidance for your company's IT employees to collect evidence themselves

Evidence may include: log files of operating systems, applications and network equipment, Internet access logs (for example, from proxy servers), network traffic dumps, hard drive images, memory dumps and any other types of information that may aid the investigation.

3

Evidence analysis

At this stage, our experts analyze all the available information (including malware, if necessary) to create a picture of the incident. Throughout the analysis and investigation, we promptly share newly discovered details so that timely action can be taken to prevent the attack from developing.

If new signs of compromise come to light during the analysis, we provide a tool to scan the company's information resources to detect other compromised hosts and collect additional data.

4

Final report

We provide you with a final report containing our findings and recommendations.

Kaspersky investigations are carried out by highly qualified cybersecurity analysts and experts. All our global expertise in digital forensics and malware analysis can be leveraged to resolve your information security incident. The service aims to:

- Isolate the threat
- Stop the attack spreading
- Search for and collect evidence
- Identify compromised resources
- Analyze the evidence and reconstruct the incident chronology and logic
- Analyze malware used in the attack (if detected)
- Analyze network and host activities
- Eliminate the threat
- Develop guidelines for restoring a healthy IT infrastructure and preventing a recurrence of similar attacks

The service is provided by our Global Emergency and Response Team (GERT)

GERT experts are certified in Incident Management, Digital Forensics, Malware Analysis, Network Security and Risk Assessment.

Expert assistance

Depending on whether or not you have your own incident response team, our experts can perform a full investigation cycle, simply identify and isolate compromised machines and prevent the spread of the threat, or perform malware analysis or digital forensics, as you require.

Results

The incident response service will eliminate the threat and provide you with a detailed report of the incident, including:

Detailed report

Brief description of the incident

In-depth incident analysis with a full timeline of events

Description of vulnerabilities used, possible attack sources, affected network components, results of malware analysis

Description of attacker actions and tools

Conclusion on the presence / absence of signs of compromise

Recommendations for mitigating any consequences of the attack and preventing such attacks from recurring

Service provision

Subscriptions are available for 1, 2, or 3 years

Kaspersky Incident Response is a subscription-based service and is available in two options: IR Retainer and IR Retainer Premium.

	IR Retainer	IR Retainer Premium
Minimum number of hours	40 hours	80 hours
How many incident responses are included?	Any quantity that can be worked out by the experts within the specified number of hours	
SLA	Standard, 24x7	Enhanced, 24x7
How Kaspersky experts work	Remote is preferable, but on site is also possible	
Can you use your retainer hours for other related cybersecurity services? If you haven't used them during the duration of your contract.	No	Repurposing is available for Threat Intelligence services: • APT / Crimeware Intelligence Reporting • Kaspersky Threat Lookup • Kaspersky Cloud Sandbox • Kaspersky Threat Data Feeds
Onboarding	You will have an introductory meeting to discuss the incident response process so that even when everything's on fire, you'll know exactly what to do	

Single-incident request

We can also help if you have a single incident request. Our experts will do their best to investigate the threat and prepare incident response recommendations quickly, but without onboarding and SLA.

Price determinants

Pricing depends on:

The number of hours

This refers to the hours required for incident response, reflecting the level of complexity and number of incidents

Type of engagement

Onsite or remotely. The remote option doesn't involve travel expenses which is why it saves time and money

Subscription type

IR Retainer with a standard SLA, or IR Retainer Premium with the highest SLA

N.B. Hours needed for the service vary from case to case.

The level of complexity is determined by our experts at the outset. Here is an example of the approximate time our experts spend on incident response, not including the time for evidence collection.

Level of complexity	Description	Turnaround time
1	One compromised machine (malware infection, data leak, financial fraud, etc.)	40-56 person-hours
2	Multiple compromised machines in the network (compromise of a particular business system, massive malware infection, compromised Active Directory domain, etc.)	56-80 person-hours
3	Complex attack leading to network compromise (complex attack in distributed networks, APT attack, etc.)	80-120 person-hours

Why Kaspersky?

The world's largest independent information security company with a global presence focused on threat intelligence and technology leadership

Several petabytes of threat data collected continuously around the world and more than two decades of expert analysis

Kaspersky's Global Emergency Response Team (GERT) is a group of experts that has been investigating complex security incidents for organizations in every industry and region for more than 10 years

Recognition

Kaspersky actively participates in independent tests and collaborates with leading global research firms. Our technologies and products are recognized worldwide and have won numerous international awards.

Proven to be the industry's most effective combination of technologies and expertise

MOST TESTED
MOST AWARDED
KASPERSKY PROTECTION
*kaspersky.com/top3

Gartner peerinsights customers' choice 2020™

Gartner Peer Insights Customers' Choice for EDR Solutions 2020 names Kaspersky Top Vendor

THE RADICATI GROUP, INC.
A TECHNOLOGY MARKET RESEARCH FIRM

The Radicati Group recognizes Kaspersky as a Top Player in the Advanced Persistent Threat (APT) Protection — Market Quadrant 2021

GERT Global Emergency Response Team

The service is provided by experts with extensive practical experience in investigating complex incidents

MITRE | ATT&CK®

Kaspersky's detection quality confirmed by MITRE ATT&CK Evaluation

FORRESTER®

Kaspersky is Positioned as a Leader in Forrester Wave™: External Threat Intelligence Services, 2021 report

About Kaspersky

Kaspersky is one of the world's largest providers of information security solutions for accurate real-time threat prediction, detection, response and elimination.

We are a key member of the top four global manufacturers of software solutions to ensure end user information security. For over 20 years, Kaspersky has been an innovator in IT security, providing effective digital security solutions for large enterprises, SMBs and consumers.

Kaspersky's technologies and solutions protect over 400 million users in almost 200 countries and territories around the world.

Let us help you protect yourself

We help you respond to and clean up incidents before they become a problem.

Learn more

Kaspersky Incident Response

www.kaspersky.com