

# Kaspersky Incident Response

[www.kaspersky.com](http://www.kaspersky.com)  
#truecybersecurity

# Kaspersky Incident Response

While your IT and security specialists work hard to ensure that every network component is both secure against intruders and fully available to legitimate users, a single vulnerability can offer an open door to any cybercriminal intent on gaining control over your information systems. No one is immune: however effective your security controls, you can become a victim.

It's becoming increasingly difficult to prevent information security incidents. But while it may not always be possible to halt an attack before it penetrates your security perimeter, it's absolutely in our power to limit the resultant damage and to prevent the attack from spreading.



Kaspersky Lab's Incident Response Services are carried out by highly experienced cyber-intrusion detection analysts and investigators. The full weight of our global expertise in Digital Forensics and Malware Analysis can be brought to bear on the resolution of your security incident.

# Malware Analysis

Malware Analysis offers a complete understanding of the behavior and objectives of the specific malware files that are targeting your organization. Kaspersky Lab's experts carry out a thorough analysis of the malware sample you provide, creating a detailed report that includes:

- **Sample properties:** A short description of the sample and a verdict on its malware classification.
- **Detailed malware description:** An in-depth analysis of your malware sample's functions, threat behavior and objectives – including IOCs – arming you with the information required to neutralize its activities.
- **Remediation scenario:** The report will suggest steps to fully secure your organization against this type of threat.

# Digital Forensics

Digital Forensics can include malware analysis as above, if any malware was discovered during the investigation. Kaspersky Lab experts piece together the evidence to understand exactly what's going on, including the use of HDD images, memory dumps and network traces. The result is a detailed elucidation of the incident. You as the customer initiate the process by gathering evidence and providing an outline of the incident. Kaspersky Lab experts analyze the incident symptoms, identify the malware binary (if any) and conduct the malware analysis in order to provide a detailed report including remediation steps.

# Delivery options

Kaspersky Lab's Incident Response Services are available:

- By subscription
- In response to a single incident

Both options are based on the amount of time our experts spend resolving the incident – this is negotiated with you prior signing the contract. You can specify the number of working hours you wish us to spend, or follow our experts' recommendations based on the specific incident and your individual requirements.

Kaspersky Lab  
Enterprise Cybersecurity: [www.kaspersky.com/enterprise](http://www.kaspersky.com/enterprise)  
Cyber Threats News: [www.securelist.com](http://www.securelist.com)  
IT Security News: [business.kaspersky.com/](http://business.kaspersky.com/)

#truecybersecurity  
#HuMachine

[www.kaspersky.com](http://www.kaspersky.com)

© 2018 AO Kaspersky Lab. All rights reserved. Registered trademarks and service marks are the property of their respective owners.

