

Kaspersky Incident Response Services

www.kaspersky.com
#truecybersecurity

Kaspersky Incident Response Services

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.



The overall aim of Incident Response is to reduce the impact of a security breach or an attack on your IT environment. The service covers the entire incident investigation cycle, from the onsite acquisition of evidence to the identification of additional indications of compromise, preparing a remediation plan and completely eliminating the threat to your organization.

We do this by:

- Identifying compromised resources.
- Isolating the threat.
- Preventing the attack from spreading.
- Finding and gathering evidence.
- Analyzing the evidence and reconstructing the incident's chronology and logic.
- Analyzing the malware used in the attack (if any malware is found).
- Uncovering the sources of the attack and other potentially compromised systems (if possible).
- Conducting tool-aided scans of your IT infrastructure to reveal possible signs of compromise.
- Analyzing outgoing connections between your network and external resources to detect anything suspicious (such as possible command and control servers).
- Eliminating the threat.
- Recommending further remedial actions you can take.

Depending on whether or not you have your own incident response team, you can ask our experts to execute the complete investigation cycle, to simply identify and isolate compromised machines and prevent dissemination of the threat, or to conduct Malware Analysis or Digital Forensics.

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
Cyber Threats News: www.securelist.com
IT Security News: business.kaspersky.com/

#truecybersecurity
#HuMachine

www.kaspersky.com

© 2017 AO Kaspersky Lab. All rights reserved. Registered trademarks and service marks are the property of their respective owners.

