Kaspersky Compromise Assessment

Identify hidden cyberthreats before they become costly breaches

~22%

of attacks stay undetected for 135 days*

Attacks detected within hours are remediated within minutes, attacks not detected for months take

> than 46 hours

to remediate*

According to MDR incidents statistics, targeted attacks actors often return to the scene of their crime**

Organizations today are faced not only with external risks, but with hidden threats within their infrastructure. Signs of compromise are not always obvious, and the way to be sure is through a Compromise Assessment service.

Your business will benefit from the Kaspersky Compromise Assessment service if:

- You believe that your network has been compromised, even though you have no obvious evidence
- A business partner has been compromised
- You're in the process of an M&A (Mergers and Acquisitions)
- According to TI data your region / industry is under risk of being attacked
- There has been a full-scale DFIR after a targeted campaign and you need to check that the attackers have not returned
- You have regulatory requirements to conduct regular compromise assessment

Kaspersky Compromise Assessment (CA) is a service that focuses on uncovering active cyberattacks as well as previous unknown attacks that have flown under the radar of your IT security tools and processes. The goal of the service is to provide high level of assurance as to whether or not your network is compromised and evaluate the overall security posture with independent expert analysis.

How Kaspersky Compromise Assessment works

Data collection

- Forensic metadata from all hosts
- SIEM logs & Active Directory
- Darknet search
- Threat Intelligence

We look at your infrastructure from different angles:

- Scan hosts and collect forensic metadata
- Analyze historical SIEM logs
- Review Active Directory configuration
- Search the Darknet for leaked credentials

Relevant data

Threat Hunting

We execute automated and manual threat hunting on all collected logs and telemetry based on unique TI data from experienced certified consultants, using our leading-edge technologies.

We identify incidents in your network and provide response recommendations.

Incidents

Incidents Validation

We conduct a forensics examination and malware analysis required for validation of detected incidents.

We develop efficient measures to scope the incident and contain the threat.

IoCs / TTPs

Report

- Includes initial incident investigation results, description of exploited vulnerabilities with security flaws which could be used by malefactors, attacks sources and network resources which were affected
- Ask the expert
- Quick-win recommendations
- Insights on the current state of cybersecurity

All-inclusive approach

kaspersky bring on the future

* Kaspersky Incident Response analyst report for 2023

** Kaspersky MDR analyst report for 2023

What we do

- Perform tool-aided endpoint scanning
- Reveal compromised systems and traces of past incidents
- Conduct detected incidents' validation to identify techniques and tools used for the attack
- Provide remediation and prevention recommendations

What you get

- A high level of assurance as to whether or not your network is compromised
- A professional, independent assessment of your security posture with an executive summary and detailed report
- Early detection of cyberattacks already in your network
- Mitigation of future damage and resulting financial loss
- Strengthening of your organization's defenses thanks to meaningful insights and actionable recommendations

Why Kaspersky Compromise Assessment?

1

Wide-ranging offering

Darknet Search, analysis of attackers' tactics, techniques and tools, validation of initial incident response and detected incidents, historical SIEM logs analysis, automated and manual threat hunting through collected endpoint telemetry with unique indicators of attacks (IoA).

2

Onsite service option

If preferred remote delivery is impossible, we can conduct the service entirely onside so your data never leaves your corporate perimeter.

3

The most comprehensive threat intelligence around

Kaspersky is a globally recognized provider of threat intelligence data in different forms with a multitude of use cases. We were responsible for remediating some of the most sophisticated state-sponsored APT campaigns in history and have been experts in operationalizing research, threat research and developing security tools for over 27 years. Our CA offering harnesses all our petabytes of accumulated threat intelligence data.

4

Unique expertise, innovative technologies

Our solutions compete with the best in the industry worldwide. Our experts are internationally experienced in every industry and are certified by GIAC, (ISC)², ISACA, Offensive Security, and others.

5

Minimal load on infrastructure and IT

We have developed a method of running our tools that doesn't create any noticeable performance impact on the CPU, RAM or network. If you use Kaspersky Endpoint for Business, there is no need to install additional agents, as the process is entirely non-intrusive.

6

Works with third-party systems

We analyze exported SIEM and other security system logs from different vendors.

www.kaspersky.com

Learn more

#kaspersky
#bringonthefuture