REMOTE INCIDENT RESPONSE KIT

Rapid forensics of Windows and Android devices

Remote Incident Response Kit

Overview

For many companies investigating a device-specific security incident, standard procedure is to remove the affected device from the network prior to reinstalling it.

Unfortunately, vital evidence regarding the cause and effect of the incident is subsequently destroyed. That leaves the organisation no wiser and, more importantly, still exposed to the same or similar attacks in the future.

Even large companies with fleshed out security teams can lack the time, human resources or an adequate data gathering tool for same-day device scanning.

Rapid and comprehensive forensics tool

Our Remote Incident Response Kit is designed to rapidly gather all security-related data from a device and to furnish incident responders with evidence. As such, the software acts as a data collector, an automated forensics backend server, and a reporting module.

Operating system compatibility

Supports all Windows-based client operating systems actively supported by Microsoft, and in all Microsoft-supported languages.

Also available for Android devices, and can be downloaded from the Google Play store.

Remote Incident Response Kit

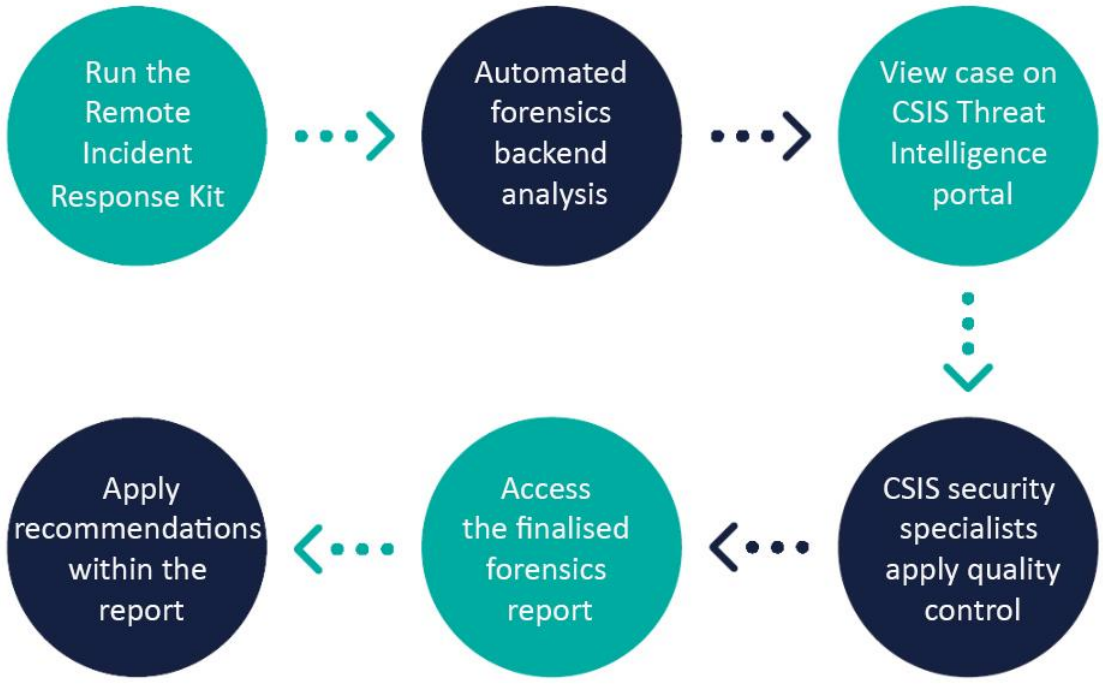
Well-suited forensics software for large organisations

For large security teams comprising professional incident responders, the Remote Incident Response Kit is an essential stand-alone tool for gathering data quickly for internal security specialists to analyse the device's artefacts for malicious activity.

Quick and easy forensics software for small organisations

For organisations that lack incident responder skills, the Remote Incident Response Kit is quick and easy to run.Thereafter, CSIS offers access to 24/7 forensics security specialists who ensure that the forensics analysis is complete and accurate, and that the correct conclusions have been drawn before recommendations are made.

Process



Key features

- Works on Windows or Android devices.
- Does not require specialist training.
- Can be executed from any software deployment tool.
- Remote scanning, from anywhere.
- No pre-installation of software required.
- Result- and recommendation-based report.

Benefits

- Understand rapidly if, how, when and with what a device has been breached.
- Comply with legal requirements by documenting and analysing security incidents.
- Save money and time by outsourcing to security specialists.
- Get 24/7 support from forensics security specialists.
- Use reports in legal proceedings or for auditing purposes.

How it works

1. You suspect a breach, and run the software to gather data.
2. The case is analysed by the automated forensics backend.
3. You view the case on the CSIS Threat Intelligence portal.

If you have an SLA with CSIS:

4. CSIS security specialists ensure the analysis is complete and accurate.
5. You access the final forensics report.
6. You act upon recommendations within the report.

The software

- Scans the device for signs of infection.
- Performs a complete memory dump.
- Creates a baseline for future comparison.
- Sends all collected data to CSIS security specialists for confirmation.

When malicious activities have been detected, the report documents:

- **when** exactly the device was infected
- **how** exactly the device was infected, and
- **what** exactly was the device has been infected with.

The reports can be used for legal proceedings, for auditing purposes, or even as crisis management background material.

Types of data collected

- Traffic Analysis
- System Diagnostics
- Suspicious files
- Browser history
- Registry backup
- AppData backup
- EventLog backup
- File timeline
- File integrity
- Memory dump

Typical use case scenarios

Scenario	Example
1. You have a security incident you want to investigate.	A device is infected with ransomware.
2. You believe a security incident has occurred and you want to investigate it.	Your browser crashes after you have clicked on a link.
3. You want to make a routine investigation	You have been to a series of conferences in the Far East.
4. You want to do “real time” threat hunting.	You run the software periodically on your organisation’s high profile targets.

CSIS Security Group A/S

Founded in Copenhagen in 2003, CSIS Security Group is a leading independent provider of cyber security services in Europe. Credited by Gartner Group for its threat intelligence capabilities, the company mitigates customers' security risk with a wide range of preventive security products and services, as well as with incident response and managed security services. CSIS is the preferred cyber security provider to some of the world's largest enterprise organisations, and is a trusted advisor to law enforcement agencies, government and news media.

CSIS Security Group A/S
Vestergade 2B, 4th floor
1456, Copenhagen
Denmark

Tel. +45 8813 6030
contact@csis.dk