CSIS

REST ASSURED.

Remote Incident Response Kit

RAPID FORENSICS OF WINDOWS OR ANDROID DEVICES

www.csisgroup.com

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
- Report based on results and recommendations

Your benefits

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

Operating system compatibility

Windows systems

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

Windows Server Windows

Android devices

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

android

Accelerated forensics

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

Vital evidence regarding the cause and effect

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.

Furnish incident responders with evidence

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.

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 smaller organisations that lack professional 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.

TYPICAL USE CASE SCENARIOS

01.

You have a security incident you want to investigate
e.g. a device is infected with ransomware.

02.

You have a suspicion that a security incident has occurred and you want to investigate it
e.g. your browser crashes after clicking on a link.

03.

You want to make a routine investigation
e.g. you have been to a series of conferences in the Far East.

04.

You want to do "real time" threat hunting
e.g. you run the software periodically on high profile targets in your organisation.

Types of data collected

- Traffic analysis
- System diagnostics
- Suspicious files
- Browser history
- Registry backup
- AppData backup
- EventLog backup
- File timeline
- Memory dump

HOW IT WORKS

01. Run
You suspect a breach and run the Remote IR Kit to gather data.

02. Analyse
The case is analysed by the automated forensics backend.

03. View Results
You view the case on the CSIS Threat Intelligence portal.

With SLA (Service Level Agreement)

04. Quality Control
CSIS security specialists ensure the analysis is complete and accurate.

05. Forensics Report
Full report including recommended actions.

06. Improve
Apply recommendations and improve your security posture.

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 are detected, the report tells you:

WHEN
the device was infected.

HOW
the device was infected.

WHAT
the device has been infected with.

Service to suit **your** needs.

YOUR CHOICE OF 3 PACKAGES

	Standard	Managed	As a service
Threat Intelligence Portal	✓	✓	✓
Statistics	✓	✓	✓
Distribution portal and guide	✓	✓	✓
Token based security	✓	✓	✓
Real-time case monitoring	✓	✓	✓
Automated forensics report **(technical)**	✓	✓	✓
Quality assured forensics report **(technical)**	-	✓	✓
Service Level Agreement (SLA)	-	72 hours	By agreement
End-user forensics report **(non-technical)**	-	-	✓
White label	-	-	Optional

White label

Branded distribution portal and guide

It is possible to have a branded distribution portal and quick guide, which can be used to easily distribute the Remote IR Kit collector to the end-customer.

The distribution portal requires a login with a 9-digit token that the client needs to enter in order to download the Remote IR Kit tool and read the quick guide.

Branded software

The Remote IR Kit collector tool can be branded with logo, support phone numbers and an EULA.

Branded end-user forensics report

The end-user forensics report can be branded with logo, disclaimers and contact/support details.

GDPR DATA BREACH REPORTING

Speed is of the essence

Upon the the discovery of a suspected security breach, GDPR-compliant organisations have just 72 hours to:

- conduct an investigation
- inform the supervisory authorities
- inform the individuals affected
- identify the breach's impact, and draft a comprehensive containment plan.

Failure to comply risks a fine of up to €20 million
(or 4% of the previous year's global revenue).

Fast forensics, less reporting

On average, our Remote Incident Response Kit takes just 3 hours to collate the data and provide a report on a suspected breach.

In the majority of cases, organisations will significantly reduce the amount of GDPR reporting required, or – if the breach alert has been triggered by a false-positive– avoids the need for GDPR reporting altogether.

REST ASSURED.

CSIS IN BRIEF

- Employee-owned Group founded in Copenhagen in 2003.
- Preferred IT security provider to some of the world's largest financial services and enterprise organisations.
- Credited by Gartner Group for outstanding threat intelligence capabilities.
- Renowned for cybersecurity advisory services and managed security solutions, as well as incident response, forensics and malware reverse engineering capabilities.

CSIS Security Group A/S

Head office
Vestergade 2B, 4th floor
1456 Copenhagen
Denmark

UK office
95 Aldwych
London, WC2B 4JF, UK

+45 88 13 60 30
contact@csis.dk

www.csisgroup.com