AGILE·**RESPONSE**·TECHNOLOGIES

THE INCIDENT RESPONSE, THREAT HUNTING AND FORENSICS PLATFORM.

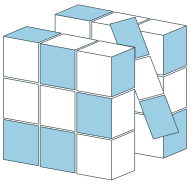
www.agileresponse.com

Cyber Breaches and Incidents Are a Reality
FOR ALL ORGANISATIONS

We have moved beyond prevention into the age of resilience.

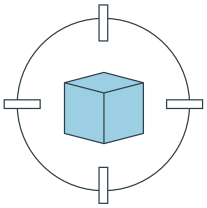
Chronos

A technological platform that assists investigators in assessing and analysing the presence and impact of cyber threats by delivering four key insights:



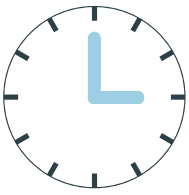
HOW...

...did the breach take place?



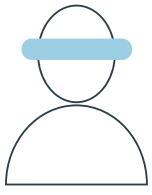
WHAT...

...data or information was exfiltrated?



WHEN...

...did the incident take place and how long did it take?



WHO...

...were the attackers and/or where were they from?

IN 2016, THE VAST MAJORITY OF ORGANISATIONS HAD A SECURITY BREACH...

90% of large organisations

▲ Up 81% from the year before

74% of small businesses

▲ Up 60% from the year before

Source: PwC - Government urges businesses to take action as cyber security breaches double, Bank of England, 2016

Whether you are an internal investigator, or an external professional that a customer has called in to help, Chronos ensures you get accurate insights quickly and efficiently, which leaves more time for action and remediation.

Ensure You Optimise Your Response to CYBER INCIDENTS

Current Approaches Are Ineffective

Much of the work done by investigators today relies either on manual approaches or a variety of oftentimes costly and difficult-to-use tools that fail to deliver accurate and reliable insights.
This means that the work of an investigator can be slow, inefficient and overly focused on basic tasks of data collection and processing, rather than on analysis, decision-making and action.

These are unfortunate facts when dealing with cybercrime because damages and losses continue to grow the longer a case remains open.

How It Works

Through a straightforward subscription aligned to your usage requirements and some initial training to get set up on Chronos, you get access to a portal through which you manage all your casework, data, analyses and reports.

There is no need to deploy any additional infrastructure in your organisation, ensuring a secure, cost-effective and reliable setup.

Generic Process

EASY DEPLOYMENT

- Case setup and collector configuration according to pre-defined parameters
- Collector: single, self-contained file that works across platforms
- Collector downloaded from secure URL and deployed to target network using existing systems

FAST COLLECTION

- Defined configuration and modules downloaded
- Modules executed in memory (i.e. does not touch disk)
- Raw data sent to back-end

▶ **Automatically done by Collector application**

EFFICIENT PROCESSING

- Parsing using custom-built modules
- Encrypted file formats decrypted and automatically appropriate parsers are run
- Indexation in large, distributed database

INTELLIGENT ANALYSIS

- Machine learning-based data correlation
- Intelligence look-ups
- Data enrichment and visualisation

AUTOMATIC REPORTING

- Easy tagging of evidence
- Automatic technical reports and management summaries

▶ **Only raw data is stored.**
Multiple copies are stored in an encrypted format.

Flexible Technology for Various USE CASES

Incident Response

When your organisation has suffered a breach, the key challenge is to provide an accurate assessment of the situation as quickly as possible. This assessment needs to be robust enough to support both technical and management decisions aimed at containing the damage, communicating actions to stakeholders and getting disrupted parts of the business back on their feet.

Chronos is ideally suited to this scenario because it:

- Allows for extremely fast collection
- Collects raw data files
- Provides broad – and constantly growing – artefact coverage
- Produces insightful reports automatically
- Can scale up to very large infrastructure
- Leaves no trace on your systems once the required actions have been completed

Threat Hunting

In our experience, most organisations have already been compromised and many may not know it yet. When you want to proactively search out cyber threats to your organisation, some of the critical success factors are about ensuring that your approach is stealthy, broad-based and high quality intelligence-driven to avoid being blind-sided on the one hand, or inundated by false-positives on the other.

Chronos is ideally suited to this scenario because it:

- Has no chance of having been corrupted or compromised through exposure to an infected network
- Can be specifically targeted and can scale up to very large infrastructure
- Is set up and run very quickly, even on extensive networks
- Is compatible with all major systems
- Draws on a powerful threat intel backbone
- Leverages Machine Learning to continuously improve its effectiveness

Forensics

When undertaking a forensic investigation, the integrity and systematic nature of the process is one of the elements of paramount importance, ensuring that findings are considered legitimate, correct and actionable.

Chronos is ideally suited to this scenario because it:

- Is a self-contained set of modules that allow the case to be executed end-to-end
- Leaves the affected environment untouched; Chronos acts on copies of the originals
- Collects raw (un-processed) data

  All data is transferred and stored in an encrypted format
- Enables easy tagging of evidence
- Is secure-by-design in its entirety: application modules, data transmission, storage
- Ensures processing time is optimised through configurable depth of analysis

The Benefits
OF USING CHRONOS

LIGHTNING FAST

Collection and processing speeds ensure you spend your time on analysis and action.

REFRESHINGLY ACCURATE

Designed by experts with deep understanding of investigative processes, IT and security. Avoid bad assumptions and false conclusions.

CRITICALLY NON-INVASIVE

Easy to deploy and remove to ensure no further disruption to your network and business.

EASY TO SET UP AND INTUITIVE TO USE

Minimal training and set up requirements mean you are up and running in no time.

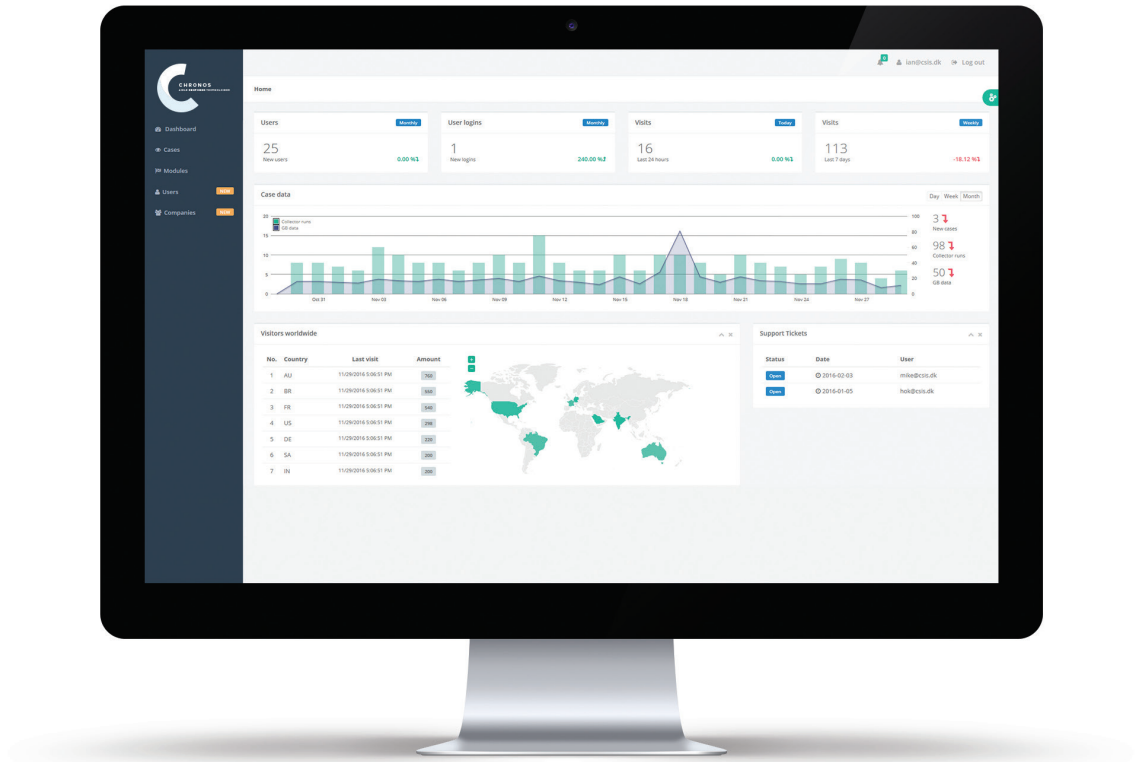
FLEXIBLY SCALABLE

Can just as easily be deployed onto a single machine or onto a large network of thousands.

ENHANCED CONTINUOUSLY

We are driving an aggressive development roadmap and constantly delivering new and improved capabilities.

The Platform Has an
INTUITIVE AND USER-FRIENDLY PORTAL



Portal Characteristics

1. Different type of user privileges – cases can be assigned to specific individuals with managers having case overviews
2. Historical and trend analysis is easily displayed in graphical format
3. Incidents, assets and cases can be geographically mapped to manage regional aspects
4. Real-time alerting is provided to the user, ensuring new actions are rapidly defined and channelled

Chronos is built for EFFICIENCY, EFFECTIVENESS AND SECURITY

Chronos Gathers Everything that Is KEY TO AN INVESTIGATION

APPLICATIONS

- All applications run

CONNECTIONS

- All connections made

FILES

- Every file touched

PLATFORMS *

ARTEFACTS (examples - not exhaustive)

- Amcache
- Application Execution Artefacts
- Chrome History
- Cookies
- Deleted Registry Keys
- Efficient Hashing with MD5, SHA1, SHA256
- Event Logs
- Firefox History
- Fuzzy Hashing
- Malware Infection Vectors
- Master File Table
- Network Information
- OS Detection
- Prefetch
- RegBack Structures
- Registry Dump
- Running Processes
- Signature Integrity Checks
- Start-up Artefacts
- User Databases
- Wifi Scanning
- Win.ini, boot.ini
- Windows Error Reporting

* Version compatibility: Windows 7 and up

CHRONOS

PROVIDING THE WORLD'S BEST CYBER SECURITY TECHNOLOGY

AGILE·**RESPONSE**·TECHNOLOGIES

Vestergade 2A, 3. sal
1456 København K

+45 4080 8100
contact@agileresponse.com

www.agileresponse.com