CSIS

REST ASSURED.

Incident Response

RETAINER AGREEMENT

www.csisgroup.com

CSIS has been working at the forefront of cyber security and cyber threat intelligence for almost two decades, and our Incident Response Team has been intimately involved with some of the most prominent and complex attacks, working hand-in-hand with our customers to identify, analyse and remediate threats.

CSIS Incident Response retainer agreement

We have developed an unparalleled understanding of both existing and emerging threat actors as well as their rapidly changing tools, tactics and procedures (TTPs).

Our world-class Incident Response Team works with the best technologies to facilitate rapid, accurate and detailed data collection and analysis, dramatically reducing the time between intervention initiation and resolution.

Hackers and malware incidents do not operate on a '9 to 5' schedule. On the contrary, most targeted attacks occur outside normal office hours in order to minimise detection.

Because of that, CSIS has implemented a 24/7 support solution, which enables you to contact CSIS any time, any day, the moment a security incident is detected.

CSIS will provide specific online support (PC deep-scans, log-file- and traffic analysis, etc.) and can provide onsite support if deemed necessary.

Benefits

- Rapid response Service Level Agreement
- Discounts on investigation tools used by Incident Response Consultants
- Reduced cost on Incident Response hours
- Dedicated phone support 24/7

> "**CSIS Incident Responders** are professional and quick to understand the problems. They have excellent interpersonal skills."

NRGi

Michael Warrer
CIO / NRGi

Get a fast response from world-class experts & rapidly reinstate full business continuity

How it works

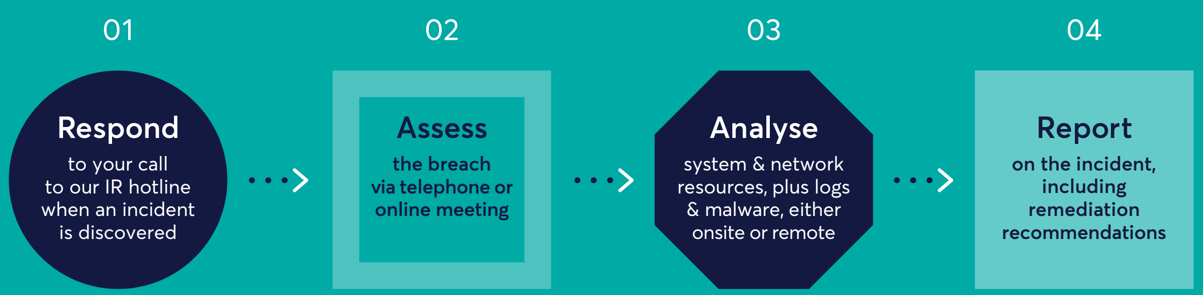
When you have a 24/7 Incident Response Retainer Agreement with us, you can call our dedicated phone number the moment a security incident is detected. Security incidents could be unauthorised money-transfers, targeted attacks, data leaks, or ransomware, amongst other types. Our first-level analyst that takes the call will take some high-level diagnostic information.

This information will be relayed to our Incident Response Team, who will set up a case and get in touch with you to initiate our incident response methodology. For a detailed review of our methodology, please see our Incident Response Consulting capabilities at:

csisgroup.com/respond-incident-response-ir

The CSIS Incident Response Team will assess the incident and provide you with a recommended course of action. The time it will take to do the assessment will vary based on the incident and information available. You may be asked to provide remote access, run detection tools (provided by CSIS) and/ or provide physical access to one or more devices on your network.

CSIS Incident Response process



01 **Respond** to your call to our IR hotline when an incident is discovered

02 **Assess** the breach via telephone or online meeting

03 **Analyse** system & network resources, plus logs & malware, either onsite or remote

04 **Report** on the incident, including remediation recommendations

We quickly determine the scope of an attack and immediately start remediation with proven techniques to secure compromised networks.

CSIS Incident Response Retainer Agreement

BE PREPARED. BE RESILIENT.

CSIS OFFERS 2 INCIDENT RESPONSE RETAINER PACKAGES

Basic & Critical

The packages have different service levels (SLA), products and services included.

CSIS IR Retainer Package	Basic	Critical
Phone support	24/7/365	24/7/365
Online support	Mon-Fri 8:30-16:30	24/7/365
Incident response start-up	Max. 8 hours	Max. 4 hours
Start-up fee	Free of charge	Free of charge
Free calls per month	1 x ½ hour	4 x ½ hour
Monitoring tools included	-	Honey Net
Investigation tools included during incident	-	LogAgent + CIRK*
Discount on use of investigation tools**	10%	15%
Discount on Incident Response hours	10%	22%

Retainer packages notes

* **5 x CIRK scans** per incident included ** **CIRK + Chronos** for incident purposes

An onboarding meeting is held to ensure a smooth start-up of the incident retainer response service. This onboarding meeting is held to gain the required understanding of the Customer's environment.

EXAMPLES OF ONBOARDING MEETING TOPICS

CSIS

- Incident handling workflow
- Walk-through of the Incident Response framework
- Training in how to use our support and what to expect

The customer

- How CSIS can expect to get access to the Company's local network
- A list of contacts to important people (incl. Management & IT)
- How local support will be provided to CSIS

SOME OF OUR INVESTIGATION TOOLS

Honey Net Monitor

CSIS Honey Net monitors has a vast collection of malicious servers and domains all over the world and analyses sinkholes for any communication from the Customer's public IP ranges. The monitor is configured to instantly warn the Customer about malicious traffic originating from their network. Warnings contain evidence of infections or data leakage and corresponding relevant metadata available through a secure web interface.

LogAgent

CSIS LogAgent is installed on the DNS server in the Customers infrastructure. The agent listens in on DNS traffic and then sends the information regarding DNS requests encrypted to CSIS. The LogAgent also makes it possible to identify internal IP addresses and network names of the clients making the DNS requests and thereby makes it possible to identify which clients in the Customer's network that might be infected.

CIRK

CSIS's Remote Incident Response Kit is designed to rapidly gather all security-related data from Windows or Android devices, to equip incident responders with evidence to do analysis. As such, the software acts as a data collector, an automated forensics backend server and it has a build-in reporting module for each collected machine.

Chronos

Chronos is a powerful incident response platform that enables our team of consultants to do mass collection of forensics artefacts across infrastructure endpoints. Through an income-parable endpoint data collection and analysis capability, the platform can analyse all hosts simultaneously to identify security threats and risks. The platform is fast and can easily scale to very large corporate networks, ensuring depth and robustness of insights, as well as, breadth of coverage.

Learn more

For more information, please contact us at **www.csisgroup.com**

CSIS

REST ASSURED.

CSIS IN BRIEF

- Founded in Copenhagen in 2003.
- Preferred cybersecurity services partner for many distinguished enterprise & mid-market companies.
- A leader in Managed Detection & Response, Cyber Threat Intelligence and Consulting Services.
- Recognised for innovation & excellence in technology development.
- Sector expertise in banking & financial services, retail & eCommerce, critical infrastructure, manufacturing, transport & logistics and government.
- Trusted advisor to national & international law enforcement agencies.
- Credited by Gartner.

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@csisgroup.com

The leader in actionable and intelligence-driven
detection and response services

www.csisgroup.com