

REST ASSURED.

Incident Response

PROFESSIONAL CALM & DECISIVENESS



CSIS Incident Response retainer agreement

- Eliminate costly delays with a pre-arranged contract
- Minimise downtime during a security incident
- Quickly identify what has happened on your systems and/or network
- Rapidly reinstate full business continuity
- Limit damages, losses & the cost of attacks
- Access security experts who understand your business
- Get advice on improvements to reduce the likelihood of further attacks.

"CSIS Incident Response
is professional and quick
to understand the problems.
Excellent interpersonal skills."

Michael Warrer
CIO / IT-Chef / NRGi **NRGi**

Minimise the duration & impact of a cybersecurity breach



Advisory Board member
of EC3 since 2013

Get a fast response from certified experts & rapidly reinstate full business continuity

How it works

When you have a 24/7/365 annual retainer agreement with us, you can call the dedicated phone number if an immediate security issue is detected (such as unauthorised money-transfers, targeted attacks, data leaks, ransomware etc.).

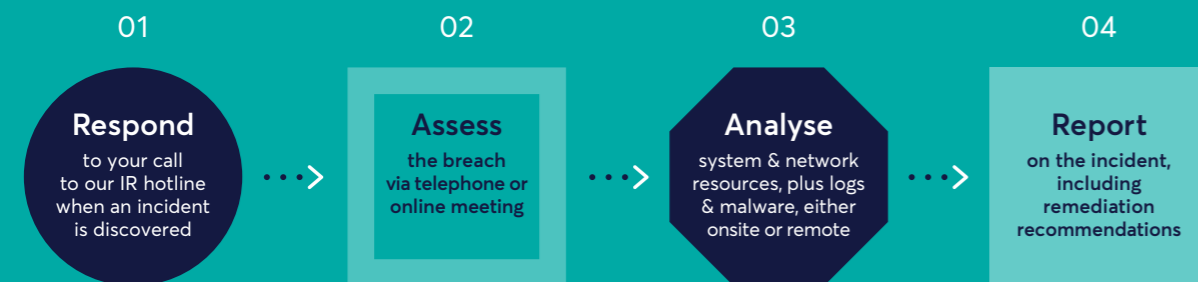
The CSIS Incident Response team will subsequently analyse the system and network resources, as well as your logs and any malware present. We then provide you with a recommended course of action.

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.

Once the threat of an incident has been mitigated, our focus shifts to eradicating all traces of the threat and recovering your impacted systems.

CSIS Incident Response process



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

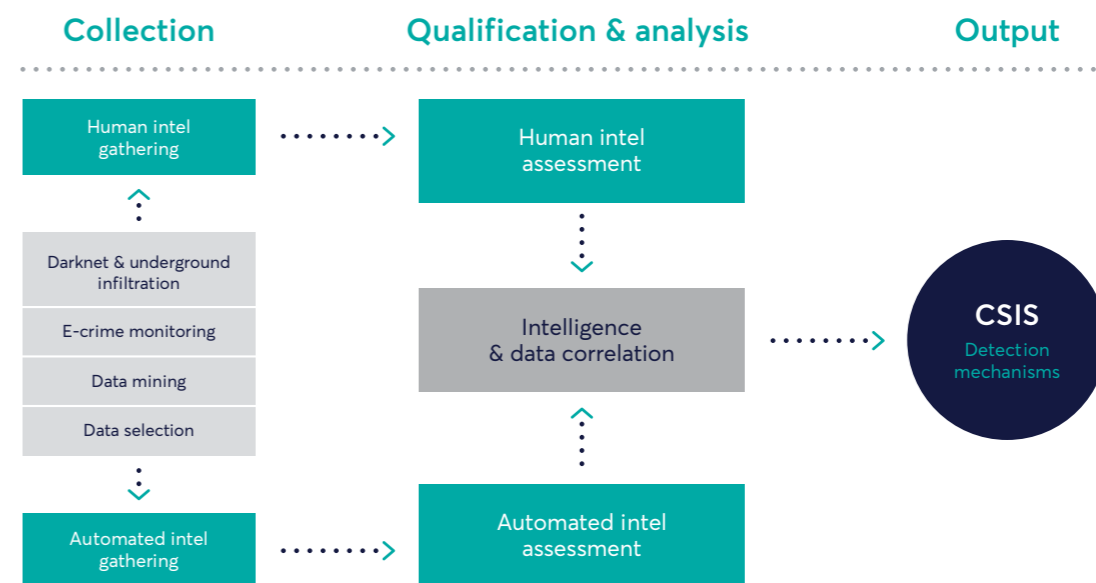
CSIS Incident Response

PROFESSIONAL CALM & DECISIVENESS

Intelligence feeds

Our real-time cybersecurity intelligence database is a collaborative network used to find cybercrime by analysing millions of domains for bot discovery, as well as malware signatures and malware-infested websites. It is automatically updated using a worldwide network of threat sensors to provide the very latest security intelligence.

Threat intelligence



- Pre-negotiated retainer service for rapid response when it matters most.
- Guaranteed response times & 24/7/365 availability.
- Real-time assistance from certified security experts.
- Tackling anything from small malware infections to advanced & persistent attacks.
- Used by some of the world largest financial institutions.

- Full audit trail & documentation of chain-of-custody, if required.
- Compliance & integration with local law enforcement (FBI, NCA, NC3, etc.).
- Compliance & integration with Europol EC3 J-CAT.
- Admissible as court evidence.
- Incident report with remediation recommendations.
- Post-event data collection & analysis.

If you've been hacked, our Incident Response experts help identify what exactly has happened to your systems and/or network, & rapidly reinstate full business continuity.

Prepare to face the challenge

Every organisation must prepare to face the challenge of responding to an event, and professional Incident Response capabilities have become an indispensable part of any effective security setup.

With an annual retainer agreement in place, you have a trusted partner to call in the event of a security breach. This proactive approach can significantly decrease response time and reduce the impact of a security incident.

YOUR CHOICE OF 3 RETAINER AGREEMENTS

Incident Reponse	Standard	High alert	Critical
Service window	Monday - Friday 8:30 - 16:30	Monday - Sunday 8:30 - 16:30	24/7/365 incl. public holidays
Start-up time guarantee	Max. 8 hours Starting within service window hours	Max. 6 hours Starting within service window hours	Max. 4 hours 24/7/365
Plantinum Alert service	Favourable subscription rate	Included	Included
Tools included	All CSIS tools	All CSIS tools	All CSIS tools + 3rd party investigation tools if required

All retainer agreements include

Incident initiation availability 24/7/365, an initial start-up meeting & an annual status update meeting.

CSIS Incident Response

Incidents handled may include, but are not limited to

- Unauthorized access.
- Data theft & recovery.
- Advanced & persistent attacks.
- DDoS attacks.
- Online fraud.
- Botnets.
- Extortion.
- Sabotage.
- Espionage.
- Financial fraud.
- Phishing attacks.
- Identity theft.
- Stolen credential repositories.
- Rogue applications.
- Intellectual property theft, & brand abuse.



Learn more

For more information, please contact us at www.csis.dk



REST ASSURED.

CSIS IN BRIEF

- Employee-owned Group founded in Copenhagen in 2003.
- 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 penetration testing, incident response, forensics and malware reverse engineering capabilities.

CSIS Security Group A/S

Head office

Vestergade 2A, 3rd floor
1456 Copenhagen,
Denmark

+45 88 13 60 30

contact@csis.dk

