CSIS

REST ASSURED.

Compromise Assessment

BE PROACTIVE
DO NOT WAIT UNTIL YOU HAVE BEEN BREACHED

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

www.csis.com

As cyber threats continue to become more pervasive, they affect companies of all sizes and across all sectors.

73% **Companies** are not prepared to respond to a cyber attack
Source: Hiscox

51% **Share of organisations** who pay the ransom after a ransomware attack
Source: Statista

287 days **Average time for companies to identify a breach**
Source: IBM

Prevent Breach Paradigm

Companies tend to build the biggest and the thickest walls to protect themselves from all forms of attacks. This process is also known as **Prevent Breach Paradigm**, though it does not hold water.

According to recent studies, it takes companies anywhere between 100 and over 250 days to detect that they have been breached. This means that attackers have plenty of time to conduct criminal activities covertly. It is worth noting that the longer the elapsed time to detection, the higher the cost of the breach will be to the affected company.

Assume Breach Paradigm

We believe that companies need to switch to an **Assume Breach Paradigm**. This change has a significant impact on the way that security is seen.

Rather than using trust in the status quo as a starting point, which can lead to high-level and sporadic checks, audits, and other types of reviews, we believe that companies should question the integrity of what they have and undertake more proactive, detailed, and ongoing reviews and exercises focused on detection and recovery.

*"I am convinced that there are only two types of companies: those that have been hacked and those that will be. And even they are converging into one category: **companies that have been hacked and will be hacked again."***

Former FBI Director, Robert Mueller

How it works

We offer **3 types of services** that drive a strong delta improvement in our customers' security postures – when combined it is a full **'Compromise Assessment'**.

01. Security Baseline Analysis

02. Threat Analysis

03. Risk Analysis

Security Baseline Analysis

A security baseline analysis looks at your attack surface and tries to reduce it to something sensible. CSIS' Security Baseline consists of several policies that help increase Customer's security posture and a set of controls that describe what is wrong and how to mitigate it.

A security baseline analysis compares your security settings against baselines from well-established and trusted organizations.

At present, we use:

- Microsoft Security Baseline
- DISA Security Baseline

Threat Analysis

Threats represent how likely the Customer is to get compromised. Malware such as backdoors, rootkits, keyloggers or advanced persistent threats give attackers a foothold in networks, which can escalate to a full-blown compromise if not removed.

Infection vectors are methods of compromising networks and are often left behind by attackers to enable them persistent access.

Our malware analysts are looking for many types of malware and infection vectors, such as:

- Trojans, viruses, rootkits
- Fake bank websites
- Fake/backdoored software
- Typosquats that have been visited by users

Risk Analysis

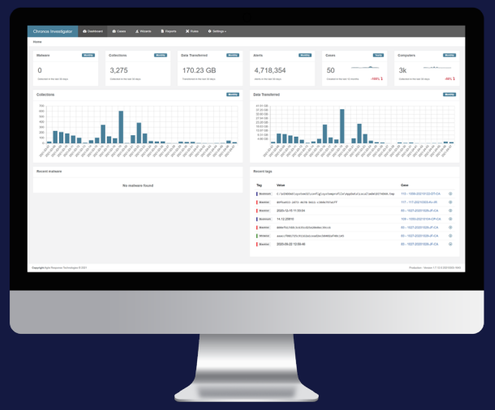
A risk is something that changes the severity of a potential breach. For example, if attackers compromise a computer through a backdoor and they find a file containing server passwords on the computer, then the backdoor is a threat, and the password file is a risk.

The password file made it much easier for the attackers to compromise the whole network, and so does many other risks. During a risk assessment, we look for exposed:

- Text files with passwords, usernames, CPR numbers, credit card details, etc.
- Shares that are writable for everyone
- Unprotected cryptographic keys
- Unauthenticated database listeners

Powered by World-Class Technology

We leverage our purpose built platform called Chronos to ensure a fast, accurate and effective service delivery process.



- Scales automates and improves every stage of the investigative process, from data collection, to analysis and reporting
- It takes minutes to run our application
- Powerful intelligence and analytics tools ensure depth and breadth of insights

Benefits

- Thorough report with prioritised findings means you know where to focus efforts
- Computer-specific findings mean you know exactly what remediation actions to take and where to do so
- Reduce the time lag between compromise and discovery and get expert input on how to mitigate issues
- Detect and respond to security threats and risks proactively
- Get additional insights through a live discussion with the team
- Engender a more proactive approach to cybersecurity

References & testimonials

"The team delivered a compromise assessment assignment for us recently. They did a great job. The project was well-managed, and we were able to easily engage with the technical team, which was highly responsive to our process and our queries. It was a demanding project due to the sheer scale of it. Most importantly, we were able to generate interesting and relevant insights through it."

Group IT Security & Risk,
Danske Bank

Danske Bank

REST ASSURED.

CSIS IN BRIEF

- Founded in 2003
- Leading pure-play cybersecurity services player
- Delivering actionable and intelligence-driven detection and response services
- Preferred partner to leading organizations across multiple sectors
- Trusted advisor to law enforcement agencies, government and news media
- Credited by Gartner

OUR OFFERING

- Managed Detection & Response (MDR)
- Cyber Threat Intelligence (CTI)
- Brand Protection
- Incident Response
- Security Consulting
- Security Software

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

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

www.csis.com