CSIS

REST ASSURED.

Security Analytics Centre

BOOST YOUR IT SECURITY POSTURE

www.csis.dk

Cyber attacks
Potential risk scenarios

- Loss of critical data
- Business interruption
- Loss of customer base
- Property damage
- Theft
- Extortion
- Brand reputation damage
- Regulatory penalties
- Loss of intellectual property
- Breach of contract
- Product recall
- Network security liability
- Notification & response costs

Today, there are **2 kinds of company**

The one that knows
it has been hacked, and
the one that's
about to realise it.

Which is yours?

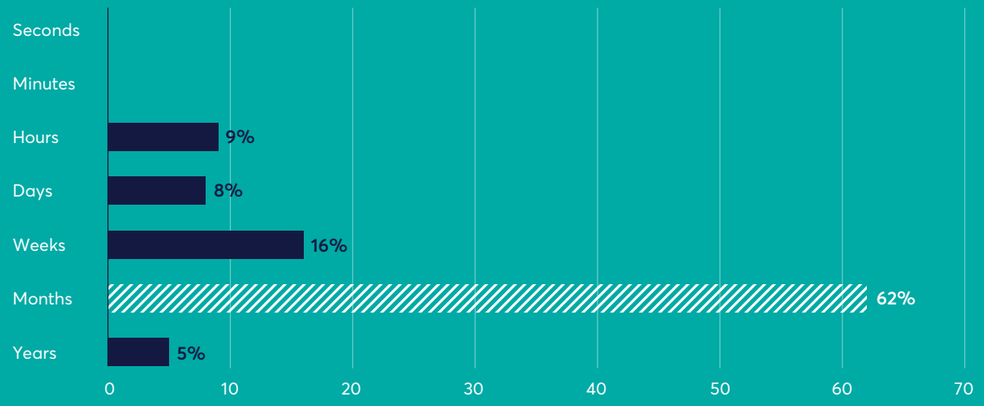
The high price of cyber-crime and business interruption

Increasing interconnectivity, globalisation, and the profitability of cyber-crime are driving a greater frequency and severity of cyber incidents, including data breaches.

Business interruption, intellectual property theft and cyber-extortion (both for financial and non-financial gain) are increasing exponentially.

The annual cost of cybercrime to the global economy is now estimated to be in excess of $445bn, with victims drawn from small, medium and large organisations.

Today, around 65% of organisations use external partners to bolster their cyber-security posture and reduce cyber-risks - up from 50% in 2013



Verizon 2014 Data Breach Investigations Report.

Three good reasons to outsource your security solution

There are 3 main reasons why outsourcing your IT security to a dedicated partner can lower your costs and optimise your security posture.

By operating security at a greater scale than your organisation, a dedicated partner is able to offer 24/7 data monitoring and incident response.

They are able to access tools, platforms and scarce IT security specialists at a fraction of the cost of developing and maintaining your own internal framework.

Critically, this allows you to release your internal resources to the areas where they can create the most business value.

Security Analytics Centre

MITIGATE YOUR IT SECURITY RISK

Exceptional threat Intelligence

Using our centralised security framework to aggregate, detect, analyse and invoke your cyber threat intelligence will strengthen your existing IT security posture and incident handling capability.

The flexible CSIS SAC solution can either be fully managed by CSIS, or we can build a hybrid solution together with your team.

Whatever the configuration, the core of the SAC is your access to industry-leading threat intelligence and security expertise, 24/7/365.

The SAC continuously develops the capability to invoke threat intelligence by correlating data patterns and matching anomalies with past events.

It is also designed to allow analysts to pivot quickly from detection to investigation, from incident monitoring and review to incident response management.

Prevent - Data monitoring

As the SAC solution gains actionable insight from possible anomalies, our analysts continuously monitor the alert queue, evaluate security alerts, and monitor the health of security sensors and endpoints.

Respond - Incident handling

For many years, we have been applying our forensics, incident handling and malware reverse engineering expertise on behalf of some of the world's largest organisations -essentially, the same skill set applied to our Security Analytics Centre.

Manage - Clear reporting

Criticality levels (ITILv3) are applied to each reported incident, helping organisations to avoid chasing "white noise" alerts and to optimise their internal resources as efficiently as possible.

Customised Security Analytics Centre solutions to meet your needs

SLA options	Standard	Business	Business Plus
Access to CSIS Security Analytics Centre	•	•	•
Secure Communication Platform for flle uploads and ticketing system.	•	•	•
Integrate & upload alerts (IDS, IPS, SIEM etc.)	•	•	•
Classification and categorization of security incidents (according to ITILv3)	•	•	•
CSIS Toolbox (Maltego transforms, incidence response kit, etc.)	•	•	•
Article database (general and in-depth cyber security news)	•	•	•
Malware infection overview of 100+ variants	•	•	•
Implementation of complete platform	•	•	•
Local technical support (phone and Email)	•	•	•
System training course / workshop	•	•	•
Security incidents handled	25	100	250
Status meetings per year (including management report)	1	2	4
CSIS intelligence feeds to SIEM or log management system (per customer)		•	•
CSIS-CERT onsite Incident Response Team			•

Access examples

Office hours only (08:30-16:30), **Nights only** (16:30-08:30), **Full Access** (24/7/365)

CSIS
Security Analytics Centre

YOUR BENEFITS

Improve your security at a lower cost

- Significantly boost your existing IT security posture.
- Access tools, platforms and scarce IT security specialists at a fraction of the cost of acquiring your own framework.
- Release your internal resources to the areas where they create the most business value.

Mitigate your IT security risk

- Reduce the risk of extortion, loss of data and theft, including intellectual property.
- Reduce infection time.
- Avoid costly disruption of your business continuity.

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

www.csis.dk