CSIS

REST ASSURED.

Secure DNS Enhanced threat protection

FAST & SIMPLE

www.csisgroup.com

Secure DNS
Benefits

- Significantly raise your security level with minimal impact on your existing IT setup
- Protect your most vulnerable infrastructure
- Minimise your administrative costs
- Complies with ISO standards
- Prevent lost revenue, lost intellectual property, and lost productivity
- Updated 24/7 with the latest threat intelligence
- Best protection/investment ratio

"It used to take days between knowledge of a threat to actual protection against it. **We now use Secure DNS to make that process a whole lot faster."**

THOMAS KAABER
IT Manager at Bang & Olufsen

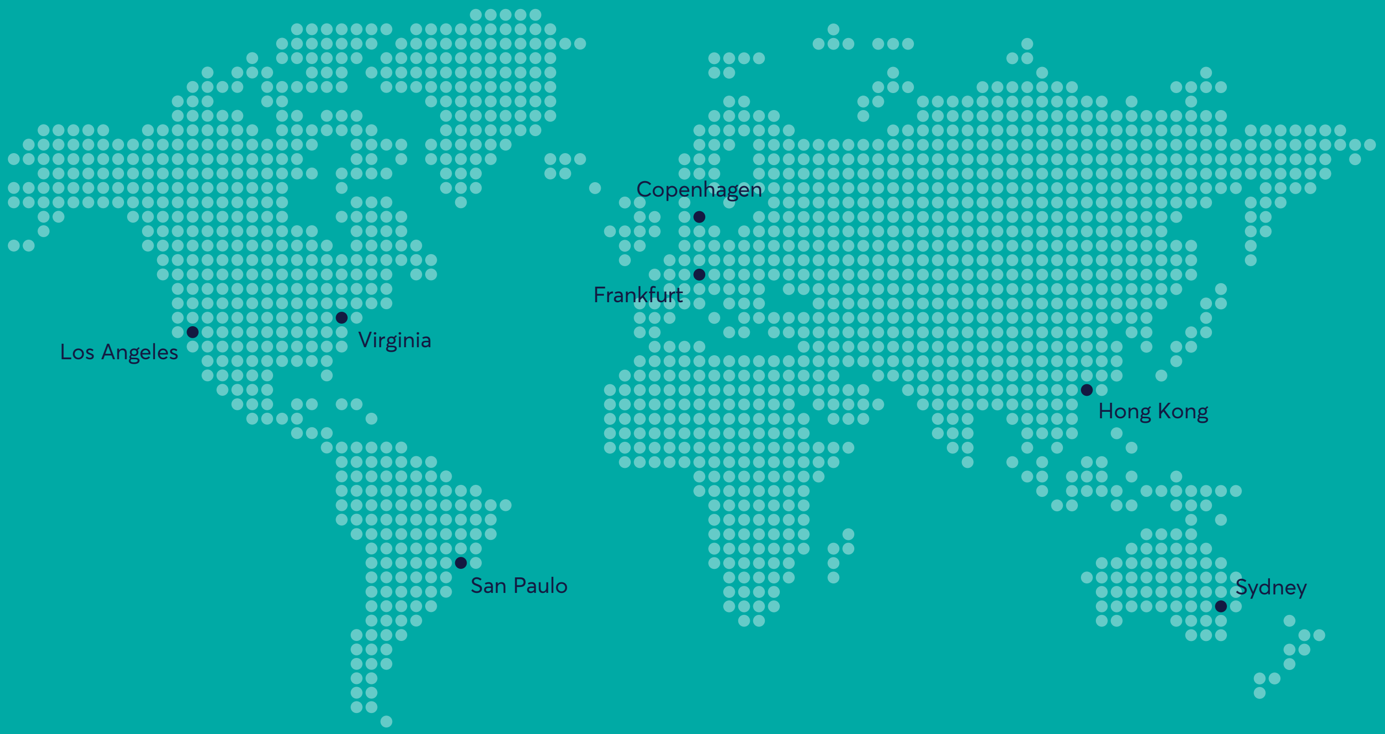
It takes awareness, focus & expertise to make so much threat intelligence available so quickly and easily.

The most comprehensive phishing and malware intelligence available in a gateway product.

Secure DNS is a network-based, intelligence-driven internet traffic protection system with the most comprehensive phishing and malware intelligence available in a gateway product, and is delivered as SaaS.

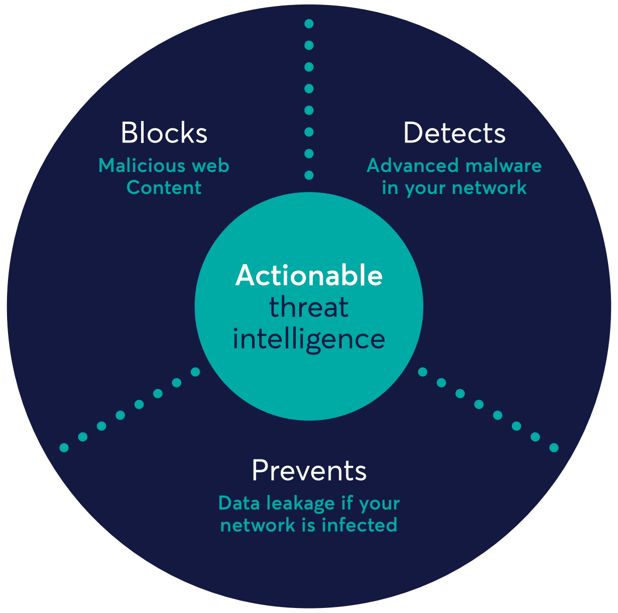
Updated with around 70,000 new malicious domains every day, the system draws upon our security analysts' extensive surveillance of hacker groups, botnets, drop-data sites, domain generation algorithms and malicious command & control servers.

Anycast locations used by Secure DNS



Secure DNS is provided globally through a secure Anycast network addressing and routing methodology.

Secure DNS Actionable Intelligence


Blocks
Malicious web Content
Detects
Advanced malware in your network
Actionable threat intelligence
Prevents
Data leakage if your network is infected

KEY FEATURES

- Add an extra layer through strong, actionable intelligence
- Detect advanced malware in your network
- Block malicious web content
- Prevent data leakage if your network is infected
- Implement in less than 15 minutes
- Instantly trace Infections to specific users and end points

> "Start collecting data. Now… Log all DNS web-proxy requests and invest in solutions that will help you ingest and analyse this data."

VERIZON 2015

Data Breach Investigations Report

Reduce your security risk

A small configuration change in the Internet-facing DNS servers of your organisation is all that's needed. You retain your existing DNS infrastructure and avoid a painful rip and replace experience.

YOUR CHOICE OF 3 EDITIONS

Secure DNS options	Basic	Plus	Managed
Detect & block web based threats	●	●	●
C&C callback blocker	●	●	●
Network based malware & APT detection	●	●	●
Data leakage prevention	●	●	●
Hosted service - no servers or client software	●	●	●
Supports all servers, desktops & mobile devices	●	●	●
Custom block and allow list	●	●	●
Basic statistics	●	●	●
Roaming client, includes CIRK scans (OPTIONAL ADD-ON)	●	●	●
Advanced statistics & forensics, with internal IP-addresses and hostnames		●	●
Secure DNS in passive/IDS mode		●	●
Customised block page (OPTIONAL)		●	●
24/7 expert analysis & alert handling by CSIS MDR team			●
Access to CSIS Remote Incident Response Kit (CIRK) for rapid forensics during an incident			●

*For Secure DNS Plus and Managed Secure DNS

A small **log forwarder** is installed on **client-facing DNS servers.**

Implement in less than 15 minutes

No downtime, service interruptions, or server reboots are needed. The service works straight away.

Implementing Secure DNS in an organisation is easy:

STEP 01.

Create account

When setting up your account, we request a list of the public IP addresses and ranges used within your organisation.

STEP 02.

Set up

With this information in hand, we set up your Secure DNS service and e-mail you instructions on how to set up your DNS forwarders.

STEP 03.

Log in

Secure DNS is now active. Log in to the web-based administration portal to check your traffic stats.

STEP 04.

Install

If you are a Secure DNS+ or Managed Secure DNS customer, you will need to install a small data collection agent on your DNS servers.

The data collection agent is required to collect information on internal IP-addresses and support Secure DNS in Passive mode (see page 15, Active and passive modes).

CSIS

REST ASSURED.

Exceptional features

Block malicious web content

The internet is becoming an increasingly bigger security threat, with more than 22% of all new domains created for illegal purposes. Your employees' day-to-day use of the internet presents a challenge because it is impossible for ordinary users to tell which sites are safe. For example, malicious code is often found in banners on entirely legitimate websites.

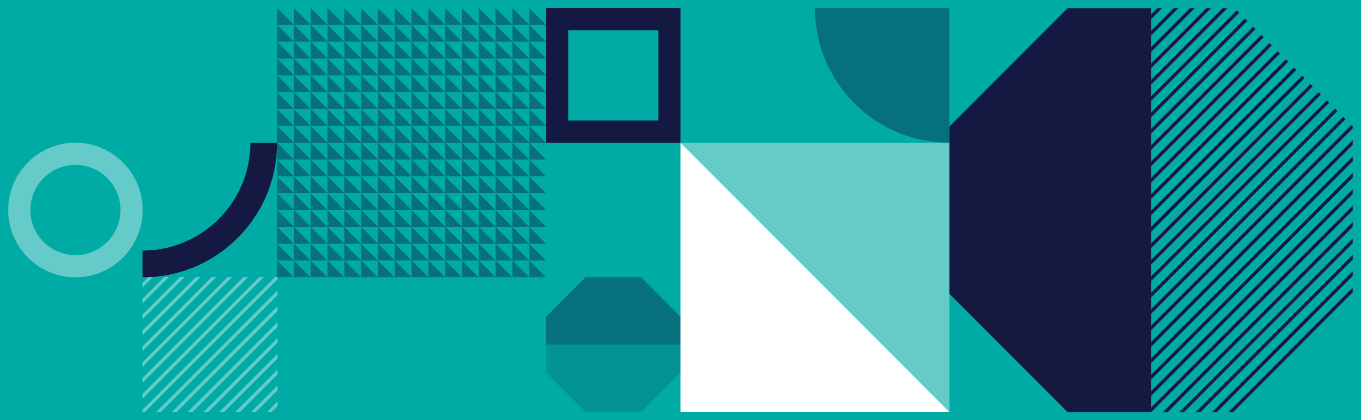
Secure DNS blocks access to websites containing malicious code, as well as servers we know to be controlled by IT criminals. Each day, we block over 20,000 new domains as part of a daily re-evaluation of over 300,000 domains.

Prevent data leakage

Secure DNS not only prevents internet-based exploits and malware downloads, it also blocks communication from existing malware intrusions and prevents them from leaking data. How? By detecting and blocking malicious traffic initiated by threats such as APT's, information stealers and ransomware.

Detect advanced malware

In addition to preventing data leakage, Secure DNS also analyses traffic to determine the infection type and identify the infected client. If an intrusion is detected, we raise an alarm and provide you with actionable data - typically with insight articles related to the infection type. Intrusion detection alerts you regardless of device type, from PC's and Macs, to Androids and iOS devices.



Exceptional features

TTL

DNS responses have a time-to-live (TTL) value. This value decides how long a given DNS pair (DNS name and resolving IP address) should be cached – typically to avoid the same DNS query being sent repeatedly when multiple machines request the same domain name.

TTL values used for malware domains are often high, which means that even though the domain is blocked at some point, it will not have an effect before the TTL value expires. Secure DNS therefore changes the TTL value for all DNS responses to a maximum of 5 minutes from the domain being blocked until it takes effect.

IP blocking

Secure DNS is able to block domains based on to which IP address it resolves. Secure DNS blocks thousands of known malicious IP addresses related to known criminal IT infrastructure. If a domain is requested and the resolving IP address is known to be malicious, the domain is automatically blocked.

Trace infections

Secure DNS logs and stores every single DNS request sent from your DNS server to CSIS's server. This allows you to search for previous DNS requests for newly discovered malware domains.

Customer use case scenarios

Using Secure DNS
to block infected offshore IT-equipment

"Our company have several offshore facilities that are not easy to maintain (e.g. re-installs, software updates, remote administration and GPO updates). Our IT equipment sometimes gets infected with malware, but because Secure DNS blocks the command & control traffic, it is not possible for the IT criminals to assume control of the infected IT equipment.

This gives us more time to fix the security concerns and sometimes, and our existing AV is eventually able to fix the security problems automatically because the malware is unable to mutate."

Using Secure DNS
to detect suspicious network patterns

"We use Secure DNS to detect suspicious network patterns in our network. These network patterns typically relate to malware traffic being blocked by Secure DNS. In theory this should only happen if we have a malware-infected device in our network.

Secure DNS alerts us each time a new suspicious network pattern is triggered, helping us to detect malware infections that have by-passed our other security measures, such as our antivirus system."

Using Secure DNS
to protect Windows XP machines

"Our company is unfortunately still very dependent on Windows XP, which is no longer supported by Microsoft.

We use Secure DNS to protect our devices against websites infected with drive-by exploit code that will try to execute malicious code on computers that are insufficiently updated."

Customer use case scenarios

Using Secure DNS
to trace state-sponsored malware

"Symantec recently warned that several energy companies could be infected with the state-sponsored malware named Havex. Unfortunately, not many AV vendors were able to detect Havex.

Once the dedicated command & control servers used by Havex became known, we could trace back in our Secure DNS log to see that none of our systems had been infected. This is possible because Secure DNS logs all DNS requests, not only those blocked."

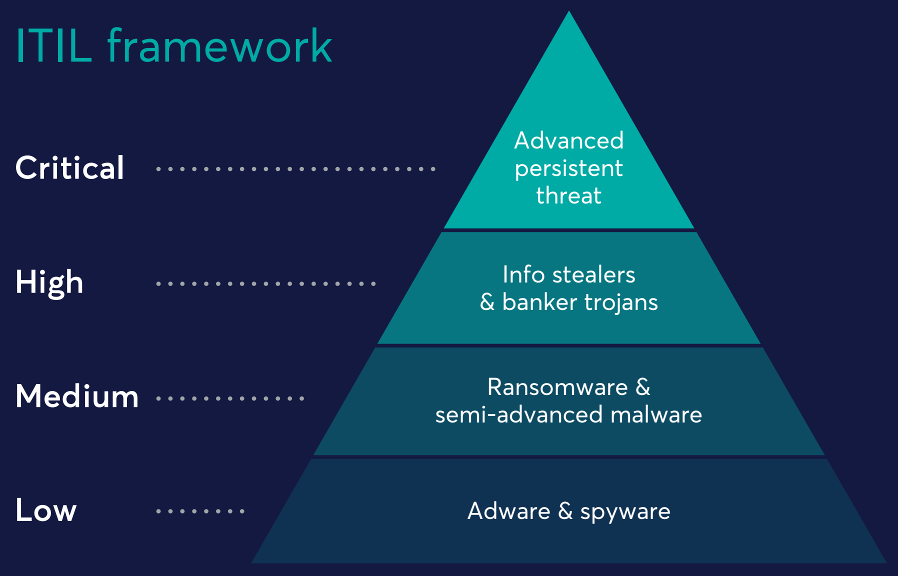
Implementing
Secure DNS in 20 minutes

"My company was heavily infected with malware undetected by our AV. We submitted a malware sample to our AV vendor, but before they could update and push new signatures, the malware had mutated again.

CSIS suggested we implement Secure DNS to mitigate the malware threat. One of their technicians guided me over the phone, and within 20 minutes, all IT-equipment within my network was protected and the malware was no longer able to mutate."

Compliance standards

ITIL framework


Critical
High
Medium
Low
Advanced persistent threat
Info stealers & banker trojans
Ransomware & semi-advanced malware
Adware & spyware

The ITIL framework forms the criticality level based on urgency and potential impact.

Criticality levels explained

Critical

Targeted attack (highly advanced malware, actively planted on the network by IT criminals).

High

Advanced malware attack (Info stealers, banker trojans, etc.).

Medium

Malware (ex: Ransomware), phishing and/or social engineering (not targeted).

Low

Adware was detected.

Info

Nothing to worry about at this stage.

Classification of a security incident

Based on the ITILv3 standard, CSIS determines the "criticality level" of a security incident based on urgency (i.e. how quickly the security incident needs to be addressed) and potential impact.

Based on the ITILv3 standard

Secure DNS helps you comply with ISO 270001/2, and security incident classifications are based on the ITILv3 standard.

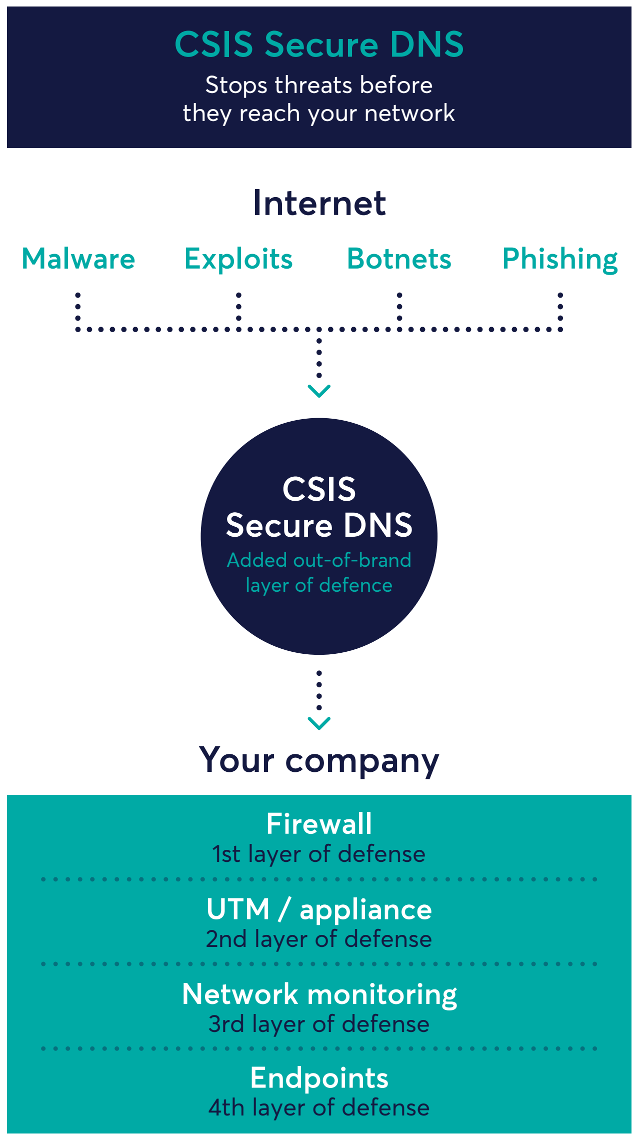
CSIS Secure DNS setup

How it fits into your network

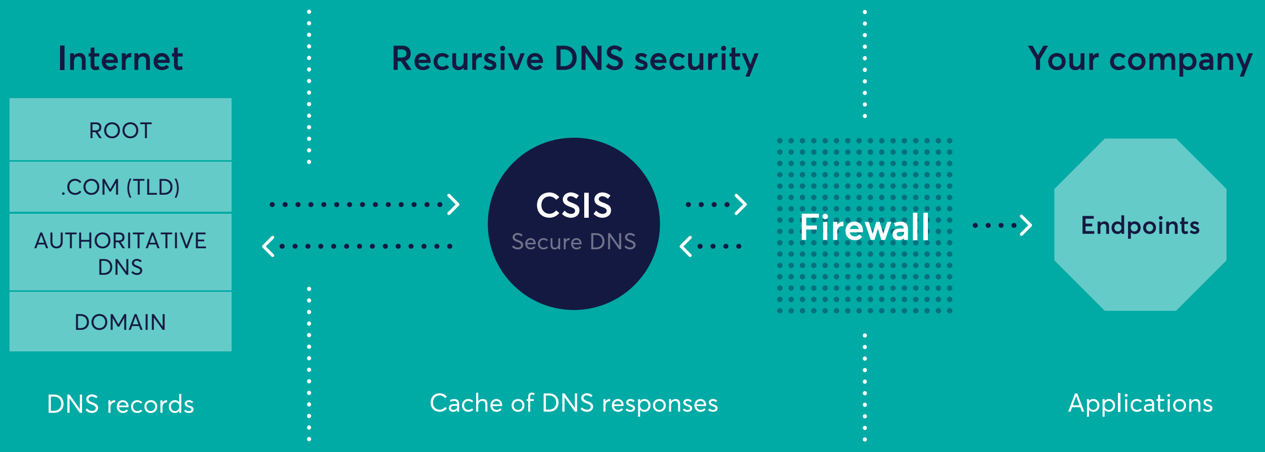
Provided that you can administer your DNS forwarders, Secure DNS works with any IT, network, or security setup in your corporation.

All you have to do to implement the service is forward DNS requests from your internet-facing DNS servers to the CSIS Secure DNS servers.

If you have multiple locations, CSIS has to know the public IP of all locations, even though all DNS queries may be routed through a central hub.



CSIS Secure DNS in the network



How it works on the CSIS side

When CSIS receives a DNS query for a blocked domain, the Secure DNS server will return our blocking IP instead of the blocked domain's IP. The client requesting the blocked domain is therefore redirected to our blocking server, which tracks the HTTP request, when possible.

When IT criminals create new domains for malicious purposes, they usually set the cache TTL to the highest possible value so that their domains 'survive' DNS blocking attempts for as long as possible. For this reason, the CSIS Secure DNS servers force the cache TTL to a maximum of 5 minutes.

When CSIS adds new domains to the Secure DNS database (or remove safe domains from it), all Secure DNS servers are synchronised within 15 minutes to ensure fast threat response, and to ensure minimum waiting time between unblocking a domain and your access to it from your network.

The Secure DNS log agent

The Secure DNS Log Agent needs to be installed on your client-facing DNS servers in order to log the internal IP and computer name of the client making the DNS query.

The Log Agent listens on UDP and TCP port 53, and copies all DNS requests sent to the server. These requests are encrypted, and sent directly to the CSIS API Server over TCP port 443.

Protect external users with the roaming client

To protect a PC outside the company network, the roaming client needs to be installed on the PC leaving the network.

The roaming client runs as a service on the PC and checks all DNS lookups that are made by the PC, using the same settings as regular Secure DNS users and logging blocked traffic. Communication is via ports 80, 53, and 443.

CSIS Secure DNS in the network

Blocking by Secure DNS

If a user browses to a domain that has been blocked by Secure DNS, he or she will be presented with the default Secure DNS blocking page. As well as informing the user that the domain is blocked, the page:

- Explains why the domain was blocked.
- Allows the user to submit a re-evaluation request.
- Provides access to the domain in safe mode.

On average, the CSIS analysists revalidate a domain within three hours after receiving a request. Safe mode presents the user with the content of the webpage in clear text only, thereby removing any harmful code that might infect the machine.

Active & passive modes

By setting your DNS forwarders to send DNS queries to our Secure DNS servers, you have engaged in Secure DNS' **active mode**, where all known malicious domains are actively blocked (as previously described).

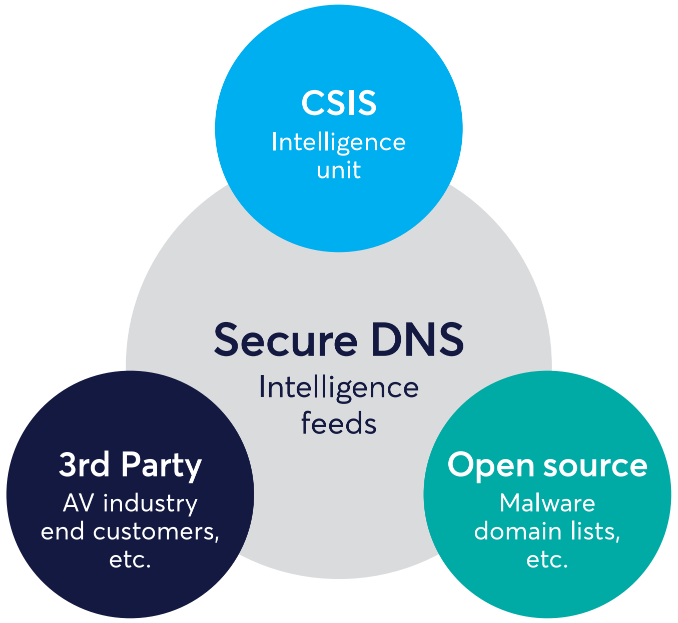
As a proof of concept, it is possible to install the Secure DNS Log Agent on your DNS servers without forwarding DNS queries to the Secure DNS servers. This results in all DNS requests being logged in our Syslog servers, without anything actually being blocked.

You can then see what would have been blocked had you forwarded DNS queries to our Secure DSN servers. We call this **passive mode**.

Threat intelligence

Intelligence source diversity

The primary driver behind Secure DNS' ability to distinguish between good and bad traffic comes from a large range of actionable threat intelligence collected from a variety of sources.



CSIS research & intelligence

Our dedicated Threat Intelligence Department comprises malware reverse engineering specialists and big data analysts. Daily work includes, but is not limited to, the following areas:

- Analysing newly discovered DGA algorithms.
- Creating new heuristics and detection filters.
- Updating website crawler detection.
- Updating feeds with intelligence from various closed malware working groups.
- Updating sandbox environments that automatically extract malware configuration files.

Threat intelligence

Open source

Open source intelligence feeds are another very important source to actionable threat intelligence.

This area covers everything from private small research feeds to large non-profit organisations that share their research.

3rd party

Cyber security threats have become increasingly sophisticated and local. IT criminals will often exploit websites within a specific country only,

and where the only users to see the malicious payload are those whose browsers have the same language settings and where the IP address matches the geography.

Secure DNS integrates with 3rd party threat intelligence feeds globally in order to cover such exploits.

Threat intelligence

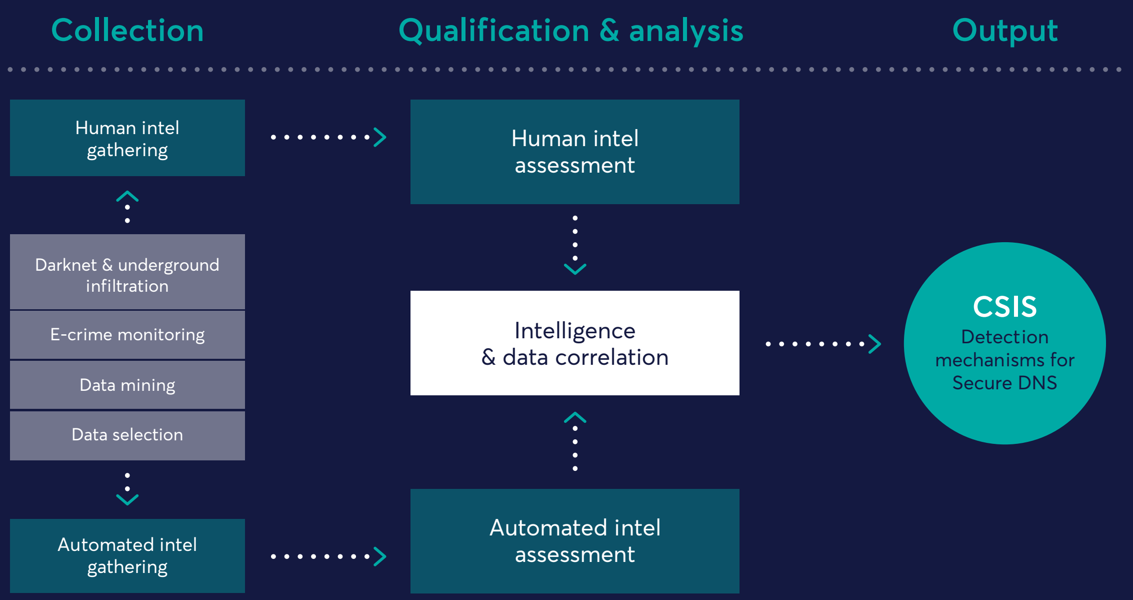
Framework & structure

Some sources are more accurate than others, and in order for all these threat intelligence sources to work efficiently, Secure DNS uses a standardised framework and structure to ensure quality assurance, continuity, and best in-class actionable threat intelligence.

Types of threats

Secure DNS distinguishes between two different threats: Prevented attacks, and possible infections.

Threat intelligence for CSIS Secure DNS


Collection
Qualification & analysis
Output
Human intel gathering
Darknet & underground infiltration
E-crime monitoring
Data mining
Data selection
Automated intel gathering
Human intel assessment
Intelligence & data correlation
Automated intel assessment
CSIS
Detection mechanisms for Secure DNS

Prevented attacks

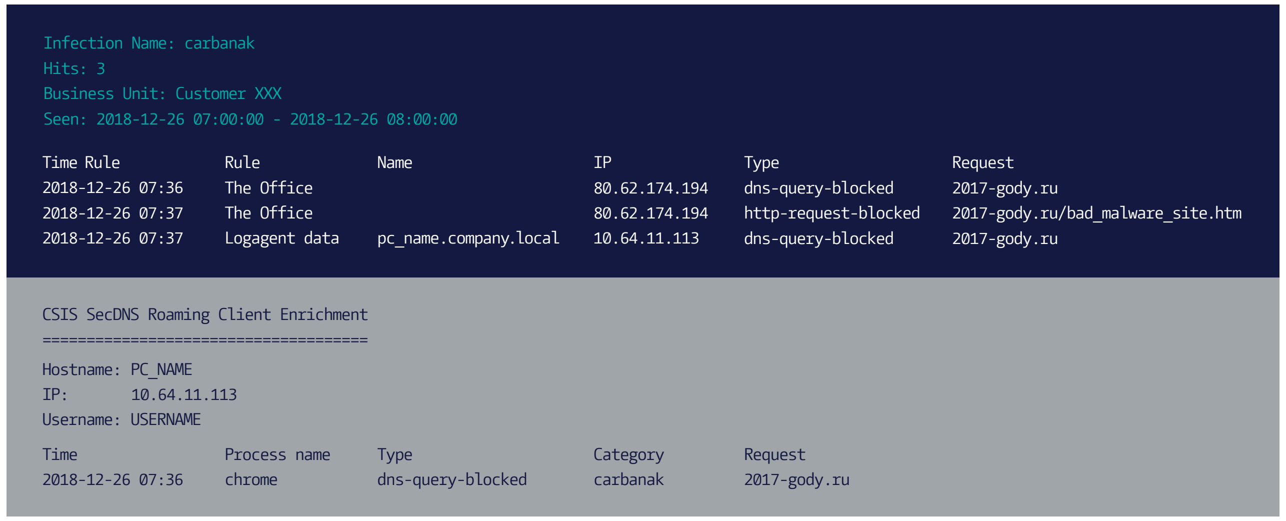
When Secure DNS prevents something from happening, such as when a user tries to visit a phishing site (but is shown a Secure DNS blocking page instead), or tries to enter a compromised website which, had it not been blocked, would have executed an exploit against the browser.

Possible infections

A strong indicator that the IT equipment that generated a particular piece of traffic is most likely infected with malware and requires attention.

Threat intelligence

Example of a Secure DNS alert



```
Infection Name: carbanak
Hits: 3
Business Unit: Customer XXX
Seen: 2018-12-26 07:00:00 - 2018-12-26 08:00:00

Time Rule         Rule          Name                  IP             Type                  Request
2018-12-26 07:36  The Office                          80.62.174.194  dns-query-blocked     2017-gody.ru
2018-12-26 07:37  The Office                          80.62.174.194  http-request-blocked  2017-gody.ru/bad_malware_site.htm
2018-12-26 07:37  Logagent data pc_name.company.local 10.64.11.113   dns-query-blocked     2017-gody.ru

CSIS SecDNS Roaming Client Enrichment
=====================================
Hostname: PC_NAME
IP:       10.64.11.113
Username: USERNAME

Time              Process name  Type                  Category       Request
2018-12-26 07:36  chrome        dns-query-blocked     carbanak       2017-gody.ru
```

The Secure DNS alert contains all the data from our logs, e.g.

- timestamp of the query
- the computer name of the machine that made the query (when possible)
- the IP of the source of the query
- the query itself, and
- which type of infection the queries are connected to.

If you have the Secure DNS roaming client installed, we will, when possible, enrich the alert with data collected from the roaming client, i.e. username of the user logged into the machine, and the process that spawned the DNS query.

You will also receive what we call historical Secure DNS alerts, where we alert you if you have queried malicious domains before we had a chance to block them. So when we add the domains to our SecDNS database, we will alert you that you queried the domain before it was blocked by us.

Types of categories

Every single piece of threat intelligence added to Secure DNS is categorized and enriched with meta data to help the user understand a given threat and take the necessary actions. Following is a list of categories added to each blocked domain:

- Manual malware
- Malware
- C&C Server
- Child abuse
- Worm
- Phishing
- Scam/Spam
- Sinkhole
- Typo-squatting
- Adware
- Drive-by exploits
- Drop server
- Mobile malware
- Virus

Threat Intelligence Portal

Alerts

An alert is generated every time someone or something in your network sends a DNS query that can be mapped directly to a specific infection (e.g. Zbot, Conficker, CryptoWall, etc.) or a specific type of infection (e.g. adware, spyware, sinkhole, etc.). This alert contains:

- Assigned severity level.
- The specific DNS query or queries.
- The HTTP request(s) when possible.
- A timestamp for each query.
- The public source IP
  (for Secure DNS Basic customers).
- Public and internal IP
  (for Secure DNS Plus or
  Secure DNS Managed customers),
  and the infection
  (or type of infection)
  that generated the DNS query.

Assigned severity levels are based on both urgency and potential impact (see Compliance, page 12).

Black & white list

Secure DNS supports a custom black and white list that allows you to overrule the blocking or non-blocking of a domain. This is to be used for security purposes only, and is limited to 100 black-listed or white-listed domains.

Management report

In order to keep track of your Secure DNS performance, we provide a management report each month highlighting the following:

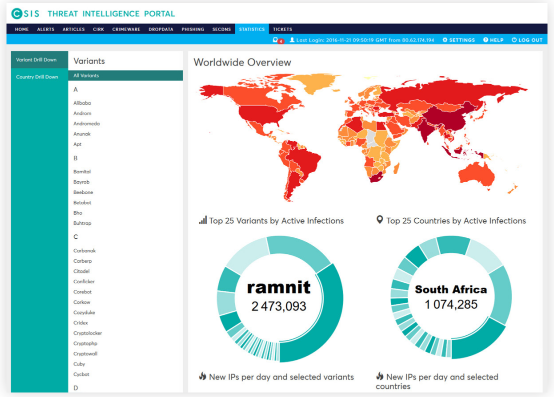
- Current threat level.
- Number of attacks prevented.
- Number of security alerts created.
- Number of new malware variants thwarted.
- Number of suspicious traffic sessions.
- Percentage of traffic blocked vs overall customer average.
- Number of threats blocked (malware / C&C servers / phishing sites).
- Internet traffic towards malicious websites.
- Top 5 threat types blocked.
- Top 5 blocked websites.
- Top 5 blocked clients.
- Top 5 visited websites.
- System up time / down time.

The portal enables you to generate a PDF report manually, should you need it.

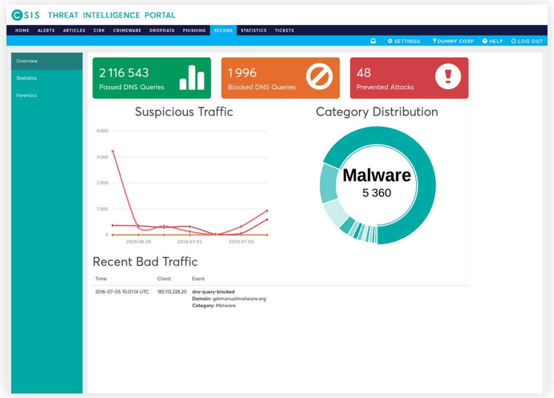
Threat Intelligence Portal

Statistics

CSIS gathers infection statistics from all over the world and presents the results in the Threat Intelligence Portal. Here you can drill down into the statistics and see which infections target a specific country, or which countries a specific infection target.



Threat Intelligence Portal
Statistics dashboard.



Recent Bad Traffic

Time	Client	Event
2016-07-05 10:01:14 UTC	185.113.228.20	**dns-query-blocked** **Domain:** getmanualmalware.org **Category:** Malware

Threat Intelligence Portal
Secure DNS overview dashboard.

Forensics trail

Secure DNS is more than just a DNS resolver. The system stores all kinds of data that is useful from a forensics trail perspective. This includes, but is not limited to:

- Blocked DNS requests
- Blocked HTTP requests
- Blocked TCP ports
- Accepted DNS requests
- Internal IP-addresses
- Domain category
- Domain malware relations

Secure DNS forensics system allows investigators to search all this data directly from the web interface. This can be useful in several different scenarios, including:

- Phishing scenario
  Determine who clicked on a specific e-mail link.
- Drive-by attack scenario
  Determine which URL the user visited just before infection.
- Malware scenario
  Clarify historical activities against a newly discovered/ reported C&C server.

Glossary

DNS-query-passed

The DNS queries resolved by the Secure DNS Server.

DNS-query-blocked

The blocked DNS queries.

http-request-blocked

Any attempt to connect to port 80 is handled by a web server. If the connection attempt is a valid http request, the web server will serve a web page explaining to the end user why the connection attempt is blocked.

TCP-syn-blocked

Any attempt to connect to the server that displays the 'Access Denied' web page. Connections to port 80 are not part of these events - they are handled by a web server.

Passed DNS queries

The total number of passed DNS queries over the past 7 days. This includes all DNS requests, including DNS requests made by specific hardware and software machines present on the customers network. Reverse lookups are also included.

Blocked DNS query

The total number of blocked DNS queries over the past 7 days.

Prevented attacks

Sums up all blocked traffic towards domains that could have resulted in an infection had you not been protected by Secure DNS (e.g. drive-by sites, binary downloader sites, etc.).

Suspicious traffic

A graph illustrating all blocked DNS and http requests over the past 7 days.

Category distribution

Showing which types of domains have been blocked over the past 7 days. The category wheel is linked to the forensics menu so that you can see the blocked DNS requests for the chosen category.

Recent bad Traffic

A list of the most recently blocked DNS requests and http requests, updated minute by minute.

Category types

Adware

Adware is a form of malware (malicious software) which presents unwanted advertisements to the user of a computer. The advertisements produced by adware are sometimes in the form of a pop-up or sometimes in a window that can't be closed. The adware category also includes banner ads known to be exploited frequently, and therefore blocked entirely.

Blacklisted

A domain blocked due to internal security policies of your organisation.

Child abuse

Child pornography is a visual representation of sexual exploitation of children, i.e. sexual violence against children illustrated on images, film or video. These are available on the internet and exchanged by people with a sexual interest in children. Production as well as distribution and possession of child pornography is considered child abuse and is punishable in most countries.

Drive-by-exploits

Drive-by-exploits infect legitimate sites that subsequently transmit malware to your computer, or change search results to direct you towards malicious sites. When visiting the website, your computer may then download unwanted programs and the like, particularly if the computer is not fully updated and patched.

Category types

Malware

Malware is a contraction of the words malicious and software. It is used as a common term for a number of categories of computer programs that do harmful or unwanted things to the computers on which they run. Malware includes computer viruses, worms, bots, trojans, spyware and adware.

Manual malware

As above, but the domains have been manually verified to distribute malware.

Mobile malware

Mobile malware is a common term for programs being harmful or doing unwanted things to the mobile device on which they run. Mobile malware includes riskware, spyware and Trojans.

Phishing

Phishing is used by computer criminals to lure personal information from users. It may include usernames or passwords for online services, online banking details, or credit card details. A common method used by computer criminals is to create fake websites that resemble legitimate websites, including bank websites.

Sinkhole

Sinkholes are domains that were originally intended for malware communication, but which have been seized by cyber security companies to monitor and track infections on a global scale. Sinkholes are not in themselves malicious, but sinkhole traffic is a strong indicator of an infection in your network.

Category types

Trojan

A trojan is a specific type of malware designed to steal personal data from a PC. One of the most common types are banker Trojans, which are designed to steal bank users' account information. These trojans have become more sophisticated and are now able to update themselves in order to expand their bank target list.

Typosquatting

Typosquatting is concerned with IT criminals who register domain names which are confusingly similar to a legitimate domain. Users who type a wrong address/URL in the browser may unintentionally visit a website that contains malicious software (malware).

Undefined

The black list used in Secure DNS is frequently updated with new domains. The updating process is partially automated, and in some instances, the data automatically received for the black list does not contain any category information.

Virus

A virus is malicious software written to misuse your computer's resources - without your knowledge or permission. A virus will often make your computer slower and even destroy important files on your computer's operating system.

Worm

A worm is malicious software written to misuse your computer's resources - without your knowledge or permission. Most worms spread through vulnerabilities such as your computer's operating system, email, or other popular communication programs.

CSIS
Customer support

CSIS

REST ASSURED.

Telephone

CSIS provides customer support in Danish and English. The phones are open Monday to Friday from 08.30 to 16.30 CET.

+45 8813 6030

Email

You can always write an email with any questions you might have, regarding the technical setup, revalidation of domains, questions regarding the Threat Intelligence Portal, etc.

support@csis.dk

Encrypted communication channel

There is also an in-built ticket system in the Threat Intelligence Portal - an encrypted communication channel between you and the CSIS Analysis team in which you can ask about specific alerts, upload suspicious email attachments, request an analysis of a malware sample, and the like.

CSIS
Secure DNS

Fast and easy implementation

- Subscription model, no initial investment needed.
- Continuous updates with no administration or maintenance.
- Fully hosted - no downtime, no service interruptions.
- No configuration changes or server reboots needed.
- Automatically covers all computers and devices in your network.

30 day trial available.

- Designed for strict eDNS compliance.
- Web-based administration interface.
- Low-maintenance, streamlined and standards-based.
- Incidents categorised using the ITIL framework.
- Employee privacy protected (only malicious data logged in detail).
- Suitable for small, medium or large organisations.

Learn more

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

CSIS

REST ASSURED.

CSIS IN BRIEF

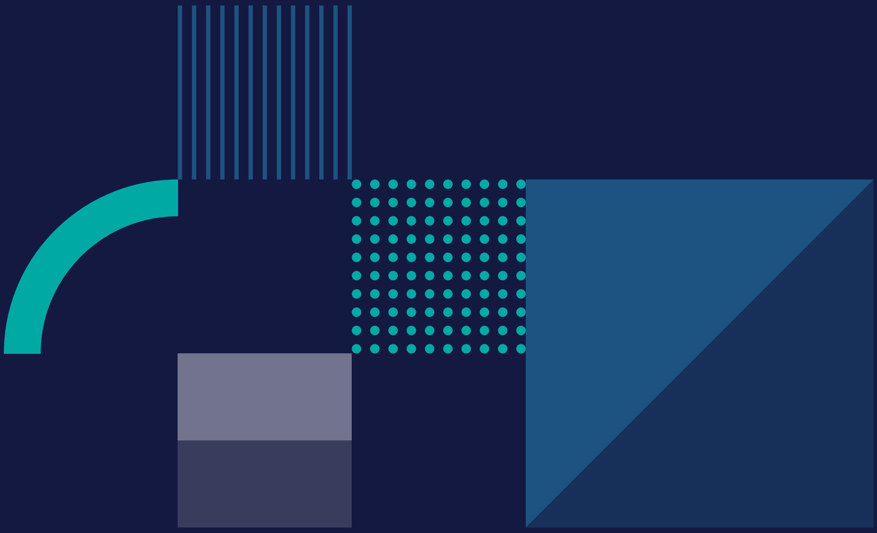
- Employee-owned Group founded in Copenhagen in 2003.
- Preferred IT security provider to some of the world's largest financial services and enterprise organisations.
- Credited by Gartner Group for outstanding threat intelligence capabilities.
- Renowned for cybersecurity advisory services and managed security solutions, as well as incident response, forensics and malware reverse engineering capabilities.

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@csis.dk



www.csisgroup.com