# Cyber Defence Feed

Malicious network traffic to and from an organisation's infrastructure can affect the business negatively in several ways including loss of data, productivity and revenue. Effective mitigation starts with a proactive approach to cyber security.

Our Cyber Defence Feed protects organisations' infrastructure against harmful connections to malicious domains and IP addresses which are under the control of cyber criminals. The risk indicators are accompanied with a confidence score ranging from 50 to 100. These scores are calculated by an algorithm based on the foundation of the extensive CSIS data platform and guided by the CSIS Cyber Threat Intelligence team's knowledge and research. Domains and IP addresses for which malicious behaviour is no longer detected are automatically removed from the feed and customer's security specialists can therefore implement an agile response against potential cyber threats.

**PACKAGES**

The feed can be obtained and accessed independently of the CSIS Threat Intelligence Portal, either as a 'push' via native integrations to selected vendors or as a 'pull' via a CSV file.

**Essential:** Consists of domains and IP addresses dedicated to malicious activities with a confidence score of 100 (maximum confidence). The feed can be ingested ('push') directly into security products (e.g. SIEM, NDR, EDR, DNS, Firewalls etc.) or a CSV file ('pull') where it can detect and/or block malicious network activity.

**Advanced:** Includes everything in the 'Essential' package including an extended data set consisting of domains and IP addresses, with a confidence score ranging from 50 to 100. The extended data set is delivered through a CSV file ('pull') and requires the knowledge and capability to set up custom rules and alerts based on the confidence scores. However, this feed contains considerably more data and as such promise a more extensive defence when implemented properly. The extended data set can be utilised in multiple ways such as directly ingested into security products, investigation during incident response handling and research.

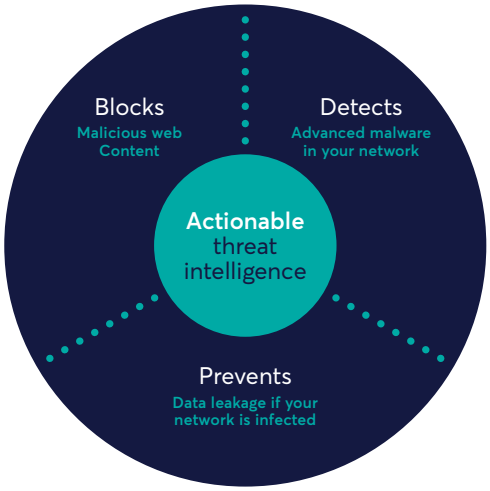
## Benefits

- Significantly raise your security level with minimal impact on your existing IT setup
- Protect your most vulnerable infrastructure
- Highly cost effective
- Prevent lost revenue, lost intellectual property, and lost productivity
- Automatically and constantly leverage our latest threat intelligence

# Actionable Intelligence

## 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




## EXCEPTIONAL USE CASES

### 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.

### Prevent
### data leakage

Our Cyber Defence Feed will not only help prevent internet-based exploits and malware downloads, it can also mitigate communication from existing malware intrusions and prevent them from leaking data. This can be accomplished by implementing the corresponding rules in the on-premise security solution.

### Detect
### advanced malware

In addition to preventing data leakage, our Cyber Defence Feed can help detect advanced malware that managed to infect network devices by circumvention of locally deployed security products. This happens because the feed data does not rely on signatures or behavior but reveals the infrastructure that the malware attempts to communicate with.

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