AbuseSA®

"We see a significant drop in vulnerable services, happier customers and more resilient networks." – ISP customer of AbuseSA

Key Capabilities

- Vendor neutral indicators
- Ingest, Harmonize and Process = Threat Intelligence
- You own your Threat Intelligence
- Automated reporting and information sharing

Proven leadership

- Long and successful track record for supporting national CSIRTs
- Brilliant method for ISPs and MSSPs to manage abuse and vulnerable services for their customers

Transparent

With transparency, you can have trust in Threat Intelligence

- Know and be in full control of your indicator sources.
- Use a clear set of rules to match indicators.

Vendor Neutral

There are no perfect sources for Threat Intelligence

- Each vendor’s view is limited.
- Vendor lock-in for indicator sources means reduced visibility.

100% Pure Intelligence – Nothing Artificial

Ingredients for a Functional Cyber Security Ecosystem

Tried and True

National CSIRTs have processed Threat Intelligence for a decade

- Their primary function is to **CLEAN** the networks
- Their secondary function to **UNDERSTAND** the situation

These organizations **COLLECT**
and **SHARE** relevant indicators
and **REPORT** incidents to victims

}

Threat Intelligence

Actionable

Actionable information is:

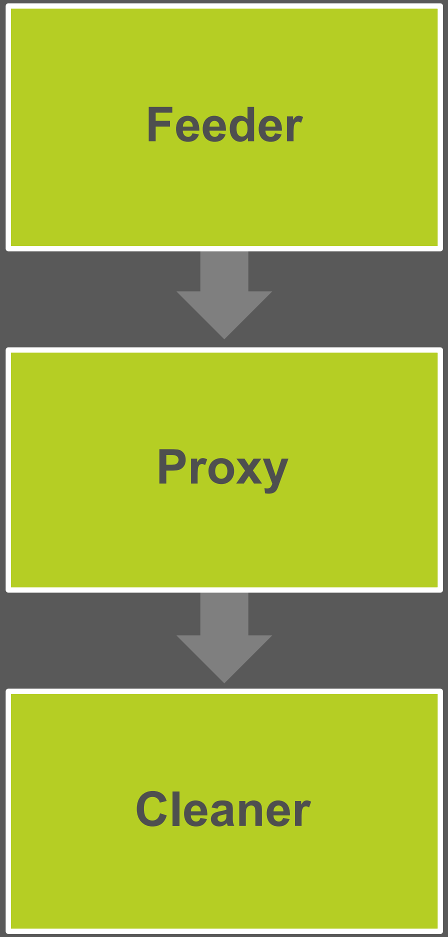
- Timely and relevant to your assets.
- Detailed enough to help the victims.
- Presented in a consistent and simple format.

External Indicators

External indicators are:

- A practical way to detect a compromise.
- Independent of you existing security investment.
- A way to keep you security vendors honest.

Threat Intelligence Ecosystem



Feeder

Proxy

Cleaner

Detection & Monitoring

Distribution & Situational Awareness

Remediation & Feedback