SYNOPSYS®

AbuseSA - Pick the Low Hanging Fruit of Protecting Your National Cyberspace

The Low Hanging Fruit

Every country strives to have their national networks clean from abuse and to protect their citizens and businesses from harm in cyberspace. A great asset to support this is the computer security community. Every day various actors report millions of observations that pinpoint compromised and vulnerable computers globally. Typically the ones at risk are regular computer users and businesses but they also include governmental bodies and critical infrastructure providers. It is a pity that large portion of these valuable observations go to waste: The information does not reach the people who would need to know.

Fixing this is truly a low hanging fruit to improve national cyber security. It gives a strong boost and practical results for any organization or authority with a national cyber security mandate. It helps internet service providers to provide better services in cleaner networks. It provides new business opportunities for forward-looking security service providers.

Start cleaning up your networks now

Synopsys can help you today with AbuseSA. It is a leading cyber threat intelligence platform specialized for automating the collection and timely sharing of actionable cyberthreat intelligence so that problems get fixed and networks get cleaned. Our technology has been in use to support national CSIRT teams to automate their network abuse incident reporting since 2009 with excellent results. We have also helped internet service providers, enterprises, cyber security authorities and defense organizations with similar goals.

ABUSESA BENEFITS

For national and domain specific CSIRTs:

- Provides robust threat intelligence feed processing and integration, with most common feeds supported out-of-the-box
- Automates victim reporting, allowing analysts to focus on advanced threats
- Provides a sound foundation for national cyber situational awareness
- Proven threat intelligence platform for national cyber defence

For Internet Service Providers:

- Interfaces with national CSIRTs and high quality threat intelligence feeds
- Automates customer abuse notifications and can integrate with customer
- Creates preemtive notifications to reduce costs associated with helpdesk functions
- Leads to better working networks and happy customers, which aids in customer retention

For Managed Security Service Providers:

- Interfaces with national CSIRTs and high quality threat intelligence feeds
- Provides better incident coverage for value-added incident response services
- Proactively communicates to customers about known breaches that their existing security measures have failed to detect
- Automates notifying customers about confirmed security incidents

Automate the whole chain

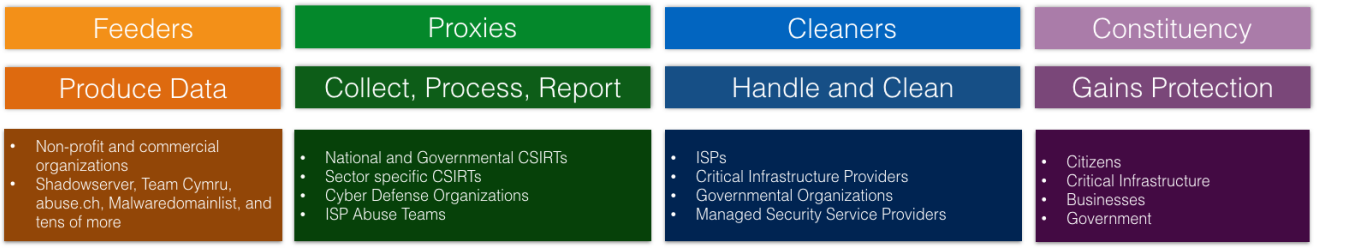
The information about incidents and victims needs to be collected from many sources, harmonised and reported automatically. AbuseSA is the platform that enables this work, having been specifically designed to cater to the needs of national CSIRTs, ISPs, and MSSPs.

For efficient country-scale network abuse reporting, the incident information needs to cross several organisation boundaries before it reaches the victim. Lack of automation in any step in the chain causes time-consuming bottlenecks that hinder the work and also allows malicious operators to gain a more long-term foothold for their operations.

AbuseSA can be used automate the whole chain, enabling near-real time victim notifications.

Actors -- Which are you?

Feeders *produce data* *which* ***AbuseSA users*** *collect, process and report systematically* *to protect their* ***constituency***



AbuseSA reference stories

True Abuse Situation Awareness through Critical Infrastructure Sector Augmentation

A national CSIRT customer of ours had been working with us to systematically define the network owners in their country. As part of this systematic work to assign critical infrastructure sectors to their stakeholders, they are able to see how abuse affects their critical infrastructure -- in real time. Recently, they had a large abuse campaign within their nation and various CSIRT teams were pulling their resources together to mitigate the abuse. At first a number of experts were debating which critical infrastructure sectors were actually affected by this campaign. Our customer, however, was able to produce a factual real-time situation picture of the campaign, since they could automatically discern the CI sectors and organizations involved.

> **Lesson learned:** *Systematic stakeholder definition and the resulting automated enriching of meta information helps gain true situation awareness over an abuse topic.*

International Real-time Sharing of Unclassified Indicators of Compromise, IOC

International automated data sharing on cyber criminality has been talked about since the 1990s. Numerous initiatives have been set up for this purpose and that never seem to get further than defining a data sharing format. With the help of AbuseSA and our public data harmonization ontology, a number of our customers are sharing CERTISP unclassified IOC, indicators of compromise, automatically, internationally and in real time. For example, NCSC-FI and CERT-UK currently use AbuseSA to share information [1].

> **Lesson learned**: *Real time automated data sharing is possible with the help of AbuseSA and its generic data harmonisation ontology.*

[1] https://www.cert.gov.uk/wp-content/uploads/2014/09/CERT-UK-adds-NCSC-FI-to-list-of-AbuseSA-feeds.pdf

SYNOPSYS®

www.synopsys.com/software

Synopsys Inc.
185 Berry Street, Suite 6500
San Francisco, CA 94107 USA

U.S. Sales: (800) 873-8193
International Sales: +1 (415) 321-5237
Email: sales@coverity.com