

RST NOISE CONTROL

RECLAIM CLARITY FROM SECURITY ALERT CHAOS

Removing known-good and well-known indicators

- **more 110 rulesets to detect known-good or well-known values, incl:**
 - MS Updates
 - CDPs
 - Popular domains
 - Well-known IPs and more
- **Supported Types:**
 - IP
 - Domain
 - URL
 - MD5
 - SHA1
- **Ready-to-use API**

Dealing with an abundance of technical Cyber Threat Intelligence (CTI) data, SOC and CTI analysts frequently face the persistent challenge of false positives. Moreover, when multiple data feeds are incorporated, this issue escalates, inundating highly skilled experts with the time-consuming task of gathering information on these indicators to confirm their status as false positives.

RST Noise Control presents a remedy for this issue, facilitating real-time validation of indicators (IP, Domain, URL, Hash) through our extensive RST Cloud noise detection engine. Our API serves to sift out irrelevant indicators and "known good" software, files and network resources, streamlining the analysis process.

Reclaim your peace of mind and decision-making clarity from the chaotic noise of security alerts, restoring your focus to the essential signals of authentic threats.

KEY BENEFITS:

- ◆ Large number of **rulesets to detect "known good"**
- ◆ **Heuristic algorithms** based on data from sandboxes and honeypots
- ◆ Real-time response via a **unified API**
- ◆ **Flexible pricing policy** with low entry

Key usage

- ◆ Decreasing false positives in real-time detection (SOAR, SIEM)
- ◆ Filtering out irrelevant data and false indicators from connected feeds (TIP)
- ◆ Integrating with custom applications

Website: <https://rstcloud.com>

Contacts: info@rstcloud.net

Trial: trial@rstcloud.net