

# [TOOL] SAM – Snort Realtime Monitor

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-02/0104.html>

---

**From:** SecuriTeam ([support\\_at\\_securiteam.com](mailto:support_at_securiteam.com))

**Date:** 02/24/05

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: 24 Feb 2005 17:16:07 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

-----

SAM – Snort Realtime Monitor

---

## SUMMARY

## DETAILS

SAM is a program to monitor (in real-time) the number of alerts generated by <http://www.snort.org/> Snort. SAM provides many ways to indicate that you may be experiencing an intrusion attempt on your network including audio/visual warnings, email warnings, etc. SAM is written in Java for maximum portability.

How can SAM alert me that my thresholds have been crossed?

SAM has many ways of grabbing your attention. The first is the rather large stop light in the top left corner of the screen. The second is by playing a specific sound when a particular threshold is reached. Currently the tool use HAL quotes, but you are welcome to change them to anything you like. They are rather obviously labeled in the sam/wav directory. The third way you can be notified is that an email can be sent to a specific person or group of persons. And lastly a plugin architecture is being planned where you can create your own creative way of alerting the appropriate people.

Sounds good. How do I run it?

On Windows you can run it by double clicking on the sam.bat file in the

Securiteam: [TOOL] SAM – Snort Realtime Monitor

top level of the directory. On \*nix boxes you can run it by executing sam from the command line (again in the main directory).

I found a bug, who do I tell?

Please visit the project page on

<<http://sourceforge.net/projects/snortalertmon>> SourceForge.

Download Information:

The tool can be downloaded from SourceForge at:

<[http://sourceforge.net/project/showfiles.php?group\\_id=59138](http://sourceforge.net/project/showfiles.php?group_id=59138)>

[http://sourceforge.net/project/showfiles.php?group\\_id=59138](http://sourceforge.net/project/showfiles.php?group_id=59138)

ADDITIONAL INFORMATION

To keep updated with the tool visit the project's homepage at:

<<http://freesoftware.lookandfeel.com/sam/>>

<http://freesoftware.lookandfeel.com/sam/>

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====

=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.