

# [TOOL] OS SIM – Security Infrastructure Monitor

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-06/0077.html>

---

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

**Date:** 06/20/05

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

Date: 20 Jun 2005 09:59:51 +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>

-----

OS SIM – Security Infrastructure Monitor

---

## SUMMARY

## DETAILS

The OS SIM project's goal is to build a working SIM (Security Infrastructure Monitor) able to integrate, qualify and correlate both high level and low level security and network events which is able to compete with commercial products recently appearing on the security market.

Integrate multiple open source security/network monitoring products to obtain three network/host visibility levels:

- \* Low level log/alert/anomaly information
- \* Mid level network risk level information
- \* High level decision support information

### Components:

- \* Spade: network anomaly detection
- \* Snort: pattern matching intrusion detection system
- \* Acid: log viewer (Event Database)
- \* Ntop: network use monitor
- \* OpenNMS: Service availability monitoring
- \* Mrtg: graphing
- \* Mysql and PostgreSQL: data storage

Securiteam: [TOOL] OS SIM – Security Infrastructure Monitor

- \* rrdtool: Round robin data storage
- \* Nessus: vulnerability assessment
- \* Nmap: Network discovery
- \* P0f: OS Fingerprinting.
- \* Arpwatch: Host – Mac.
- \* More to come....

To download the tool please visit:

[http://sourceforge.net/project/showfiles.php?group\\_id=86016&package\\_id=89233](http://sourceforge.net/project/showfiles.php?group_id=86016&package_id=89233)  
[http://sourceforge.net/project/showfiles.php?group\\_id=86016&package\\_id=89233](http://sourceforge.net/project/showfiles.php?group_id=86016&package_id=89233)

ADDITIONAL INFORMATION

The information has been provided by <mailto:dkarg@users.sourceforge.net>  
Dominique Karg.

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

<http://sourceforge.net/projects/os-sim/>  
<http://sourceforge.net/projects/os-sim/>

=====

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.