Prelude-LML - Feature #397

OSSEC log & prelude-lml rule

03/02/2011 03:36 PM - Vladimir Lapshin

Status:	Closed	**Start date:**	03/02/2011
Priority:	Normal	**Due date:**	
Assignee:	Thomas ANDREJAK	**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:			
Resolution:			

Description

Hello!
I have logs OSSEC in this format:

something
timestamp
something
log record

something
timestamp
something
log record

...etc.

Tell me please, how I can attach timestamp to the log entries? Give an example please.
Thank you!

History

#1 - 03/02/2011 03:38 PM - Vladimir Lapshin

Log format:

something

timestamp

something

log record

#2 - 05/29/2016 04:26 PM - Thomas ANDREJAK

- Status changed from New to Closed

- Assignee set to Thomas ANDREJAK

You can use Prelude-LML context or the IDMEF connector in OSSEC.