Prelude Manager - Feature #125

log to syslog as well

01/22/2006 07:11 PM -

Status:	Closed	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:	Yoann VANDOORSELAERE	**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:	0.9.2		
Resolution:	invalid		

Description

If syslog output was provided alerts could be processed though SEC (simple event correlator) will no effort. This would allow for very powerful processing of alerts.

Otherwise, basic SEC rules should be provided for the XML log format.

History

#1 - 01/22/2006 07:40 PM -

- Status changed from New to Closed

- Resolution set to invalid

I don't think that adding syslog output for this one purpose would be worthwhile.
However, after looking over the SEC information at http://kodu.neti.ee/~risto/sec/, I'm intrigued by the idea of using SEC to provide correlation capabilities to Prelude, so I'll explore using it in conjunction with the XML output, then see what I can do about getting it fed back into Prelude-Manager.

#2 - 01/22/2006 10:10 PM - Yoann VANDOORSELAERE

Moreover generated syslog line would end up being very long due to the number of available IDMEF fields, which would break one of the syslog requirement that line should be no longer than 1024 characters.

#3 - 04/29/2009 12:27 PM - Yoann VANDOORSELAERE

- Project changed from PRELUDE SIEM to Prelude Manager

- Category deleted (3)

- Target version deleted (0.9.2)