ThreatFactor NSIA - Feature #150

Logging Improvements

05/11/2010 02:07 PM - Luke Murphey

Status:	Closed	**Start date:**	05/11/2010
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	100%
Category:		**Estimated time:**	0.00 hour
Target version:	0.9 (Beta)		

Description

The CEE message format requires some changes to make the log easier to use:

- Add a severity field with the name of the severity
- Add spaces between the fields
- Change category to something that better describes the field for message type (such as name)

History

#1 - 05/11/2010 02:09 PM - Luke Murphey

See http://www.splunk.com/base/Documentation/4.1.2/Knowledge/UnderstandandusetheCommonInformationModel for CIM details

#2 - 05/11/2010 03:52 PM - Luke Murphey

Additionally, need to make sure that all log fields use the same case (some are upper-case but should be lowercase)

#3 - 05/12/2010 10:44 AM - Luke Murphey

- Target version set to 0.9 (Beta)

#4 - 05/13/2010 07:15 PM - Luke Murphey

- % Done changed from 0 to 30

Changed formatting of field names to lowercase with underscores in r456.

#5 - 05/13/2010 07:52 PM - Luke Murphey

- % Done changed from 30 to 60

Added space between fields in CEE messages in r457

#6 - 05/13/2010 08:04 PM - Luke Murphey

Category should probably be event (and category_id should be event_id)

#7 - 05/13/2010 08:13 PM - Luke Murphey

Added severity description to CEE formatted log messages in r458.

#8 - 05/14/2010 01:06 AM - Luke Murphey

- Status changed from New to Closed

- % Done changed from 60 to 100

Changed event log field "category" to "event" in r460.