Prelude-LML - Feature #206

Knowing the ruleset id generating alerts

03/22/2007 11:50 AM - Sebastien Tricaud

Status:	Closed	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:	Yoann VANDOORSELAERE	**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:	0.9.9		
Resolution:	fixed		

Description

It is currently impossible to know the ruleset id that generated the alert. This is a very valuable information.

History

#1 - 04/03/2007 06:04 PM - Yoann VANDOORSELAERE

- Status changed from New to Assigned

There are two solutions to this problem, either add the ID to an additional_data field, otherwise use classification.ident. However, the later is only valid if we are 100% sure that rules can not generate alert for multiple classification. Ramon is the LML ruleset maintainer, he might have interesting opinion to share on this topic.

#2 - 04/27/2007 07:13 PM -

I'll opt for doing it in additional_data. It's probably a good idea to add the revision in there, too.
In this case, the id and rev keywords lose their purpose, so a ruleset change of this type would require all the rules to be touched (which isn't a problem, just stating it)

#3 - 04/28/2007 10:21 AM - Yoann VANDOORSELAERE

- Status changed from Assigned to Closed

- Resolution set to fixed

(In r9391) Add rule ID and revision for each rule that match, within [[AdditionalData]]. Fix #206.

#4 - 04/28/2007 10:24 AM - Yoann VANDOORSELAERE

Certain rules using variable classification.text, we wouldn't be able to use the ID as classification.ident since IDMEF state:

```
      The "ident" attribute value MUST be unique for each particular
      combination of data identifying an object, not for each object.
      Objects may have more than one "ident" value associated with
      them.  For example, an identification of a host by name would
      have one value, while an identification of that host by address
      would have another value, and an identification of that host by
      both name and address would have still another value.
      Furthermore, different analyzers may produce different values for
      the same information.
```

Although this specific issue could be fixed, there is also another issue with alert generated from multiple rules, through context. Since we want to record all matched rules ID and revision, using [[AdditionalData]] should be the way to go.

This has been implemented in r9391.

#5 - 04/29/2009 12:27 PM - Yoann VANDOORSELAERE

- Project changed from PRELUDE SIEM to Prelude-LML

- Category deleted (4)

- Target version deleted (0.9.9)