Prelude-LML - Bug #213

LML rulesets should be updated to use IDMEF Action

04/03/2007 05:31 PM - Yoann VANDOORSELAERE

Status:	New	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:	Prelude OSS 5.1.0		
Resolution:			

Description

Current rulesets (except modsecurity) does not make use of the IDMEF Action class.

```
4.2.6.2.  The Action Class

   The Action class is used to describe any actions taken by the
   analyzer in response to the event.
   category

      The type of action taken.  The permitted values are shown below.
      The default value is "other".  (See also Section 10.)

   +------+-------------------+-----------------------------------------+
   | Rank | Keyword           | Description                             |
   +------+-------------------+-----------------------------------------+
   |    0 | block-installed   | A block of some sort was installed to   |
   |      |                   | prevent an attack from reaching its     |
   |      |                   | destination.  The block could be a      |
   |      |                   | port block, address block, etc., or     |
   |      |                   | disabling a user account.               |
   |      |                   |                                         |
   |    1 | notification-sent | A notification message of some sort     |
   |      |                   | was sent out-of-band (via pager,        |
   |      |                   | e-mail, etc.).  Does not include the    |
   |      |                   | transmission of this alert.             |
   |      |                   |                                         |
   |    2 | taken-offline     | A system, computer, or user was taken   |
   |      |                   | offline, as when the computer is shut   |
   |      |                   | down or a user is logged off.           |
   |      |                   |                                         |
   |    3 | other             | Anything not in one of the above        |
   |      |                   | categories.                             |
   +------+-------------------+-----------------------------------------+

      The element itself may be empty, or may contain a textual
      description of the action, if the analyzer is able to provide
      additional details.
```

History

#1 - 04/03/2007 05:45 PM -

- Status changed from New to Assigned

#2 - 04/29/2009 12:27 PM - Yoann VANDOORSELAERE

- Project changed from PRELUDE SIEM to Prelude-LML

- Category deleted (4)

- Target version deleted (93)

#3 - 04/30/2009 01:25 PM - Yoann VANDOORSELAERE

- Target version set to 0.9.15

#4 - 09/23/2013 10:52 AM - Jean-Charles ROGEZ

- Assignee deleted (59)

- Target version changed from 0.9.15 to 121

#5 - 11/08/2015 12:01 PM - Thomas ANDREJAK

- Target version changed from 121 to Prelude OSS 3.0.0

#6 - 04/23/2016 07:49 PM - Thomas ANDREJAK

- Target version changed from Prelude OSS 3.0.0 to Prelude OSS 3.1.0

#7 - 09/28/2016 11:15 PM - Thomas ANDREJAK

- Status changed from Assigned to New

- Target version changed from Prelude OSS 3.1.0 to Prelude OSS 4.0.0

#8 - 09/19/2017 12:40 PM - Thomas ANDREJAK

- Target version changed from Prelude OSS 4.0.0 to Prelude OSS 4.1.0

#9 - 12/23/2018 11:10 PM - Thomas ANDREJAK

- Target version changed from Prelude OSS 4.1.0 to Prelude OSS 5.0.0

#10 - 12/23/2018 11:37 PM - Thomas ANDREJAK

- Target version changed from Prelude OSS 5.0.0 to Prelude OSS 5.1.0