Libprelude - Bug #14

sensor.c API rework

06/03/2004 11:16 AM - Yoann VANDOORSELAERE

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

Description

Need to clean up the mess in sensor.c, use a per sensor object instead of using global everywhere. Cleanup and review the interface.

#11 and #12 depend on this ticket.

History

#1 - 06/06/2004 11:49 PM -

- Status changed from New to Assigned

#2 - 06/08/2004 12:25 PM - Yoann VANDOORSELAERE

This is what we came up to after some discussion, comment are greatly appreciated, flames will goes to /dev/null.

```
1. Configuration files changes



/etc/prelude-sensors/ -> /etc/prelude/
/etc/sensor-name/ -> /etc/prelude/sensor-name/
/var/spool/prelude-sensors/ -> /var/spool/prelude/

/etc/prelude-sensors/sensors-default.conf -> splitted in two part:
  /etc/prelude/defaults/global.conf included by everyone (agents, sensors, managers).
  /etc/prelude/defaults/manager-client.conf included by agents and sensors.
```

- Some definitions:
  - sensors: monitoring application sending events to a manager.
  - managers: application receiving sensors events, and possibly relaying theses events to others manager.
  - agents: application connected to a manager, issuing specific task depending on the manager input (correlation agents, counter measure agent).

```
2. API renaming



- Need to encapsulate sensor.c API in an object.
  - This object is used by agents/managers/sensors, and the behavior vary depending on the type
    - prelude_client_t seem to encapsulate all of the above.
      - conflict with existing prelude_client_t connection API, which should be renamed
```

#3 - 06/10/2004 11:52 PM - Yoann VANDOORSELAERE

- Status changed from Assigned to Closed

- Resolution set to fixed

#4 - 06/10/2004 11:53 PM - Yoann VANDOORSELAERE

Fixed in changeset r3717

#5 - 04/29/2009 12:26 PM - Yoann VANDOORSELAERE

- Project changed from PRELUDE SIEM to Libprelude

- Category deleted (1)