ThreatFactor NSIA - Bug #12

Errors from Event Log Hooks After Upgrading

04/08/2010 10:24 PM - Luke Murphey

Status:	New	**Start date:**	04/08/2010
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:	Log Management	**Estimated time:**	0.00 hour
Target version:			

Description

Event log hooks cannot survive an upgrade to a new version of NSIA because they are serialized and native Java serialization fails with newer versions of the classes.

Related issues:

Related to ThreatFactor NSIA - Feature #17: Email Action Improvements	**New**

History

#1 - 04/08/2010 10:29 PM - Luke Murphey

Event log hooks should probably be replaced with a system that acts on scan results directly as opposed to older method of hooking into the event log events. A system that acts on scan results would have the following benefits:

- Could aggregate on repeated failures (only report once per day, hour, etc)
- Have site-group, rule and global scopes
- Include more information about the detection in the escalation

#2 - 04/08/2010 10:31 PM - Luke Murphey

Note, there is no built-in way to delete hooks that can no longer be loaded. You have to delete them from the database directly.

This isn't necessary though since the old hooks don't prevent the application from running correctly (just generate log messages indicating that they could not be loaded).

#3 - 11/02/2010 01:09 PM - Luke Murphey

- Category set to Core Application

#4 - 11/02/2010 01:09 PM - Luke Murphey

- Category changed from Core Application to Log Management

#5 - 01/22/2011 09:19 AM - Luke Murphey

A couple of options for handling this:

1. Purge event log hooks that will not load during upgrade operations
2. Give users an option to purge event log hooks that fail to load (like a debug console or command-line option)

#6 - 07/23/2014 09:37 PM - Luke Murphey

- Assignee deleted (Luke Murphey)