ThreatFactor NSIA - Feature #73

Definition File Loading of Custom Signatures

04/08/2010 11:59 PM - Luke Murphey

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

Description

The system for loading definitions should be capable of determining if the definitions provided are custom or official.

1. If official, all existing official definitions should be deleted before loading the new set
2. If custom, then only the definitions that are not official should be removed

This will allow the official definitions to be used in concert with a custom definition set.

History

#1 - 04/09/2010 12:00 AM - Luke Murphey

To fulfill this request, the definition loading mechanism must:

- Distinguish between official and custom signatures
- Implement a loading mechanism to delete the correct set of signatures (custom or official)

It distinguish between custom and official definitions, the following methods may be employed:

- Use different extensions
- Encrypt the official definitions file
- Have an argument in the XML that indicates that the definitions are official

Once the definitions are uploaded, the system must import import the definitions according to the description below:

Rule Types	Description
Official	Remove all official definitions, then add new ones
Custom	Replace each definition that matches the given name

#2 - 04/09/2010 12:01 AM - Luke Murphey

All definitions are now assigned IDs. This may make this ticket easier to action.

Below are some notes on how it works:

- Definitions without unique identifiers will be loaded at startup. the interface blocks them but the system will be allowed to load in order to prevent an error state that cannot be recovered from.
- The interface includes a suggested ID based on the next available ID. A message is given indicating that the ID is a duplicate if it is already taken when the user saves the definition. the message includes a suggestion for the next available ID.

- The definition still contains the "local ID". The local ID is the unique key that the definition has in the database.

#3 - 11/02/2010 01:18 PM - Luke Murphey

- Category set to Scan Engine