Prelude Correlator - Feature #363

prelude-correlator: spamhaus drop plugin

09/10/2009 03:37 PM - Anonymous

Status:	Resolved	**Start date:**	09/10/2009
Priority:	Low	**Due date:**	
Assignee:	Yoann VANDOORSELAERE	**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:	0.9.0		
Resolution:			

Description

this is a replica of the dshield plugin, but for the spamhaus drop list. it does require the use of some other python packages for CIDR lookup; so keep that in mind when merging (see attached patch).

double check the installation settings; this was my first attempt at that too.

Associated revisions

Revision 6ee57df6 - 09/15/2009 08:50 AM - Wes Young

Initial SpamhausDrop plugin implementation (closes #363)

History

#1 - 09/11/2009 11:30 AM - Yoann VANDOORSELAERE

Hi Wes, thanks for the patch!

Here is a quick review:

- The NetCIDR modules have been deprecated in favor of the more widely available netaddr module, check http://oubiwann.blogspot.com/2008/08/netaddr-python-library.html

- The __ipNormalize() function could be removed since it is now unused.

- Could you please add the Dshield plugin copyright, adding your contact to the author lists ?

This is a nice addition, thanks for the contribution!
Might you post an updated patch?

#2 - 09/13/2009 09:16 PM - Anonymous

- File spamhausdrop-patch.txt added

re-formulated. They don't have all the features in netaddr that NetCIDR had (at least that's what they said in the doc), but given that it's all but deprecated I just added a few lines using the new netaddr packages and tested it. Appears to work OK.

all the other stuff added as requested.

#3 - 09/14/2009 11:42 AM - Yoann VANDOORSELAERE

- File 0001-added-spamhausdrop.py-to-plugins.patch added

Thanks for the update!

Attached is a modified version of your patch, that provides compatibility with earlier netaddr module version, use IPSet() in order to match addresses, and download the initial database on source distribution generation.

Could you please let me know if this modified patch doesn't break anything on your side?
Thanks!

#4 - 09/14/2009 11:54 AM - Yoann VANDOORSELAERE

- File 0001-added-spamhausdrop.py-to-plugins.patch added

#5 - 09/14/2009 11:54 AM - Yoann VANDOORSELAERE

- File deleted (0001-added-spamhausdrop.py-to-plugins.patch)

#6 - 09/14/2009 03:49 PM - Anonymous

Just tested it in our QA environment; looks OK to me.

#7 - 09/15/2009 08:49 AM - Yoann VANDOORSELAERE

- Project changed from PRELUDE SIEM to Prelude Correlator

- Category deleted (generic)

#8 - 09/15/2009 08:52 AM - Yoann VANDOORSELAERE

- Status changed from New to Resolved

- Assignee set to Yoann VANDOORSELAERE

- Target version set to 0.9.0

Thanks! Plugin checked into the GIT repository.

Files

0001-spamhaus-drop-list-plugin.patch	5.29 KB	09/10/2009	Anonymous
spamhausdrop-patch.txt	4.57 KB	09/13/2009	Anonymous
0001-added-spamhausdrop.py-to-plugins.patch	9.51 KB	09/14/2009	Yoann VANDOORSELAERE