Prelude Correlator - Bug #383

Correlation of multiple different security events

06/22/2010 08:43 AM - axl axl

Status:	Closed	**Start date:**	06/22/2010
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:			
Resolution:	invalid		

Description

Hello! I need help in writing a plugin for prelude-correlator which will correlate 2 or 3 alerts. For example I want prelude-correlator to generate a correlation-alert if 3 ICMP Packet matched alerts are detected and then a remote login is attempted against the same destination IP. Thank you very much!

History

#1 - 02/08/2012 08:08 PM - Francois POIROTTE

- Tracker changed from Support to Bug

Est-ce qu'on veut traiter ce genre de demandes ? J'aurais tendance

#2 - 02/16/2012 07:20 PM - Thomas GIRARD

Je confirme : on est en best effort, pas de maintenance

#3 - 07/22/2014 11:06 AM - Antoine LUONG

- Status changed from New to Closed

- Resolution set to invalid