QFQ - Feature #6299

Attack detection: log table with invalid SIP access

23.06.2018 18:32 - Carsten Rose

Status:	Some day maybe	**Start date:**	23.06.2018
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:	next4	**Spent time:**	0.00 hour
Discuss:			

Description

Die Abwehrmassnahmen fuer SIP brute force sollen wie folgt verbessert werden.

- Es gibt eine Tabelle die alle mis-hit auf SIP oder Persistent SIP notiert:
  - IP
  - PHP Session
  - feUser
  - UserAgent
  - pageId
  - Zeitpunkt
- QFQ prueft bei jedem Start ob ein Full Stop (Attack detected) noetig ist:
  - Hits pro Sekunde, pro Minute, pro 5 Minuten, pro Stunde, pro Tag, pro Monat
  - Count pro IP, count pro PHP Session, count pro feUser
  - Fuer jede 'Hit/pro Zeit'-Klasse gibt es einen Schwellwert.
  - Ist der Schwellwert ueberschritten, wird die IP gesperrt, resp. die PHP Session gesperrt.
  - Eintraege aelter als einen Monat werden geloescht.
- Es wird nicht erwartet das viele Daten in der Tabelle stehen.

Related issues:

Related to QFQ - Feature #3947: Attack detectect: logout current user	**Some day maybe**	**24.06.2017**

History

#1 - 23.06.2018 18:32 - Carsten Rose

- Related to Feature #3947: Attack detectect: logout current user added

#2 - 11.12.2019 16:02 - Carsten Rose

- Status changed from New to Some day maybe