Prelude-LML - Feature #315

Using Named variables in PCRE ruleset

09/13/2008 08:42 PM -

Status:	New	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:			
Resolution:			

Description

Named Variables in pcre:

This would make for quicker and simpler rules to be created in prelude-lml.

Example from ntsyslog.rules:

```
regex=security\[success\] 528 (.*) Successful Logon:  User Name:(?<username>[\w ]+)  Domain:(?<dom
ain>.+)  Logon ID:\(?<lid>.*\)  Logon Type:(?<ltype>\d+)  Logon Process:(?<lprocess>\w+) .* Workst
ation Name:(?<wks>\S+);
    classification.text=Login; \
    classification.reference(0).origin=vendor-specific; \
    classification.reference(0).meaning=Windows Event ID; \
    classification.reference(0).name=528; \
    classification.reference(0).url=http://www.ultimatewindowssecurity.com/events/com189.html; \
    id=1401; \
    revision=3; \
    analyzer(0).name=NTsyslog; \
    analyzer(0).manufacturer=ntsyslog.sourceforge.net; \
    analyzer(0).class=Logging; \
    assessment.impact.severity=low; \
    assessment.impact.completion=succeeded; \
    assessment.impact.type=user; \
    assessment.impact.description=$username successfully logged on on $wks ($domain domain) via $l
type; \
    source(0).process.name=$5; \
    source(0).node.address(0).category=unknown; \
    source(0).node.address(0).address=$wks; \
    source(0).node.name=$wks; \
    source(0).user.category=os-device; \
    source(0).user.user_id(0).type=current-user; \
    source(0).user.user_id(0).name=$username; \
    target(0).user.user_id(0).type=current-user; \
    target(0).user.user_id(0).name=$username; \
    additional_data(0).type=integer; \
    additional_data(0).meaning=Logon type; \
    additional_data(0).data=$ltype; \
    additional_data(1).type=string; \
    additional_data(1).meaning=Authentication domain; \
    additional_data(1).data=$domain; \
    last
```

History

#1 - 09/13/2008 08:43 PM -

Sorry forgot to use my email address.

#2 - 09/15/2008 03:13 PM - Yoann VANDOORSELAERE

Implementing named variables would ease ruleset writing, but I am curious about the performance impact it would have. Could you write a small

performance test, to compare the speed of captured string retrieval using index/variable?

#3 - 04/29/2009 12:21 PM - Yoann VANDOORSELAERE

- Project changed from PRELUDE SIEM to Prelude-LML

- Category deleted (4)

- Target version deleted (93)

#4 - 04/30/2009 01:25 PM - Yoann VANDOORSELAERE

- Target version set to 0.9.15

#5 - 09/23/2013 10:49 AM - Jean-Charles ROGEZ

- Target version changed from 0.9.15 to 121

#6 - 11/08/2015 12:00 PM - Thomas ANDREJAK

- Target version changed from 121 to Prelude OSS 3.0.0

#7 - 04/23/2016 07:50 PM - Thomas ANDREJAK

- Target version changed from Prelude OSS 3.0.0 to Prelude OSS 3.1.0

#8 - 05/29/2016 04:27 PM - Thomas ANDREJAK

- Target version deleted (Prelude OSS 3.1.0)