Website Monitoring - Bug #1656

App doesn't support FIPS mode

12/18/2016 02:50 AM - Luke Murphey

Status:	Closed	**Start date:**	12/17/2016
Priority:	Normal	**Due date:**	
Assignee:	Luke Murphey	**% Done:**	100%
Category:		**Estimated time:**	0.00 hour
Target version:	2.0.1		

Description

History

#1 - 12/18/2016 02:55 AM - Luke Murphey

https://answers.splunk.com/answers/481420/does-website-monitoring-app-work-with-fips-140-2-m.html

#2 - 12/21/2016 06:47 AM - Luke Murphey

http://docs.splunk.com/Documentation/Splunk/6.5.1/Security/AboutusingSSLtoolsinWindowsandLinux#About_FIPS

```
Before you start Splunk Enterprise for the first time, edit $SPLUNK_HOME/etc/splunk-launch.conf to add the fol
lowing line:

SPLUNK_FIPS=1
```

#3 - 12/21/2016 06:47 AM - Luke Murphey

Might want to have a unit test for this

#4 - 01/05/2017 10:29 PM - Luke Murphey

Unit tests passed when running locally. Will try on the CI environment now.

#5 - 01/05/2017 11:26 PM - Luke Murphey

CI unit tests pass. I might need to improve test coverage to include looking for the hashes.

#6 - 01/06/2017 12:44 AM - Luke Murphey

I'm seeing an error when I run the app:

```
fips_md.c OpenSSL internal error, assertion failed: Digest update previous FIPS forbidden algorithm error igno
red Aborted (core dumped)
```

What is odd is that the unit test don't detect this because running "splunk cmd python" doesn't run Python in FIPS mode. The following works on a FIPS Splunk instance:

```
import hashlib
hashlib.md5("test").hexdigest()
```

Neither hashlib.algorithms_available nor hashlib.algorithms_guaranteed indicate that MD5 is not available even in the code running with OpenSSL in

FIPS mode.

#7 - 01/06/2017 12:45 AM - Luke Murphey

Ok, it looks like it is set in an environment variable.

```
import os
print os.environ.get('SPLUNK_FIPS', '0')
```

#8 - 01/06/2017 12:47 AM - Luke Murphey

I tried running the unit tests with the environment variable set. It didn't work. As far as I can tell there is no way to run the units tests in FIPS mode.

#9 - 01/06/2017 02:15 AM - Luke Murphey

https://bugs.python.org/file17970/py3k-hashlib-fips-issue9216.patch

Might be able to use this code to determine if OpenSSL is in FIPS mode too.

#10 - 01/06/2017 07:48 PM - Luke Murphey

- Status changed from New to Closed

- % Done changed from 0 to 100