Raporlama Modülleri

Raw analiz sonuçları işleme modülleri tarafından işlendikten ve soyutlandıktan sonra (bkz. Processing Modülleri), Cuckoo tarafından mevcut tüm raporlama modüllerine iletilir. Bu modüller, küresel konteynere erişir ve farklı formatlarda erişilebilir ve tüketilebilir hale getirir.

Başlarken

Tüm raporlama modülleri, `cuckoo/cuckoo/reporting/` dizini içine yerleştirilmelidir (bu, `cuckoo.reporting` modülüne çevrilir).

Her modül ayrıca `$CWD/conf/reporting.conf` dosyasında özel bir bölüme sahip olmalıdır: örneğin, `cuckoo/cuckoo/reporting/foobar.py` adında bir modül oluşturursanız, `$CWD/conf/reporting.conf` dosyasına (ve böylece Git deposundaki `cuckoo/data/conf/reporting.conf`) aşağıdaki bölümü eklemelisiniz:

```
[foobar]
enabled = on
```

Sizin bölümünüze eklediğiniz her ek seçenek, raporlama modülünüzde self.options sözlüğünde kullanılabilir olacaktır.

Çalışan bir JSON raporlama modülü örneği aşağıdadır:

```
import os
import json
import codecs

from cuckoo.common.abstracts import Report
from cuckoo.common.exceptions import CuckooReportError

class JsonDump(Report):
    """Saves analysis results in JSON format."""

    def run(self, results):
        """Writes report.
        @param results: Cuckoo results dict.
        @raise CuckooReportError: if fails to write report.
        """
```

```
        try:
            report = codecs.open(os.path.join(self.reports_path, "report.json"), "w",
"utf-8")
            json.dump(results, report, sort_keys=False, indent=4)
            report.close()
        except (UnicodeError, TypeError, IOError) as e:
            raise CuckooReportError("Failed to generate JSON report: %s" % e)
```

Bu kod basitçe, işleme modülleri tarafından üretilen küresel konteyneri alır, JSON'a dönüştürür ve bir dosyaya yazdırır.

Geçerli bir raporlama modülü yazmak için birkaç gereklilik vardır:

- `Report` sınıfından alan bir sınıfınızı bildirin.
- Ana işlemleri gerçekleştiren bir `run()` fonksiyonunuz olsun.
- Mümkünse çoğu istisnayı yakalamaya çalışın ve bir sorunu bildirmek için `CuckooReportError` istisnasını yükseltin.

Tüm raporlama modülleri, bazı özniteliklere erişime sahiptir:

- `self.analysis_path`: ham analiz sonuçlarını içeren klasörün yolu (örneğin, `storage/analyses/1/`)
- `self.reports_path`: raporların yazılması gereken klasörün yolu (örneğin, `storage/analyses/1/reports/`)
- `self.options`: `conf/reporting.conf` dosyasındaki raporun yapılandırma bölümünde belirtilen tüm seçenekleri içeren bir sözlük.

Revision #1
Created 19 January 2024 11:59:41 by Ertan Sözer
Updated 19 January 2024 12:00:53 by Ertan Sözer