Metrics Calculation and Datasources

Normalization of Periodic Events

Some of the following metrics rely on events over a period of time ie. M1 relies on BGP leakage events. The basic idea of how we calculate the metric is then:

> Create incidents from continuous events and weight them based on their combined duration. Note that *only events that share the same weight can form an incident.*

More specifically:

An **incident** is considered to be one or multiple events that happen at the *same time span*. These events could happen at the same time and/or may also be a chain of events. The weights for all events is by default `1.0`. Events have a lower weight when they are of less importance ie. the ASN participating in the event is more hops away from the event's culprit.

Each incident is normalized based on duration and weight like so:

- 0, duration == 0;
- 0.5 * weight, duration < 30 mins;
- 1.0 * weight, duration < 24 hours;
- 1.0 * weight * 2, penalty for every 24 hours.

The final score is then the sum of the incidents' individual score.

M1

M1 normalizes the periodic events for which the ASN was the culprit of BGP leakage events.

Statistics available for this metric: mean, median.

The datasource used for this metric is bgpstream.

M1C

M1C is closely related to M1 and normalizes the periodic events for which the ASN was an accomplice (the ASN was present in the AS-PATH reported with the event) to BGP leakage events.

The further away an ASN is from the culprit on the AS-PATH the less the weight on the calculation would be.

Statistics available for this metric: mean, median.

The datasource used for this metric is bgpstream.

M2

M2 normalizes the periodic events for which the ASN was the culprit of BGP hijacking events.

Statistics available for this metric: mean, median.

The datasource used for this metric is bgpstream.

M2C

M2C is closely related to M2 and normalizes the periodic events for which the ASN was an accomplice (the ASN was present in the AS-PATH reported with the event) to BGP hijacking events.

The further away an ASN is from the culprit on the AS-PATH the less the weight on the calculation would be.

Statistics available for this metric: mean, median.

The datasource used for this metric is bgpstream.

M3

M3 normalizes the periodic events for which the ASN was the culprit of BGP bogon advertisement events.

Note that the duration of each incident is counted per day as the data on CIDR report report only on a daily basis.

Statistics available for this metric: mean, median.

The datasource used for this metric is CIDR report.

M6

M6 checks if the ASN has a sufficiently registered policy. The check is the following:

```
m6 = the ASN has at least 1 import and 1 export registered
```

Statistics available for this metric: mode.

The datasource used for this metric is ripestat.

M7IRR

M7IRR calculates the percentage of the registered routes of an ASN. The calculation is the following:

```
m7irr = % of registered routes
```

The calculation considers as total routes all the advertised routes in BGP. More specific unregistered routes that are advertised but are covered by a less specific registered route are also considered registered.

Statistics available for this metric: mean, median.

The datasource used for this metric is ripestat.

M8

M8 checks if the ASN has registered contact information. The check is the following:

```
m8 = the ASN has registered contact information
```

Abuse contact information is not taken into account for this metric.

Statistics available for this metric: mode.

The datasource used for this metric is ripestat.