Standard Categories for Incident Response Teams

Joint Metrics V2.1

January 2018

Introduction

To help standardise incident response metrics across different entities (for example UK Academic Institutions), it has been suggested that there is a standard number of incident response categories, which each entity agrees to use when collating data. As each entity has agreed to the definition of each category, the metrics across entities can be directly correlated and each entity can determine their exposure to a category on a monthly basis (depending on how often the metrics are collected).

This document should be read in conjunction with the definitions found in;

Standard Categories for Incident Response Teams (Definitions)

Definitions

For the purposes of this document, the following definitions are used;

Entity: an institution / company which collects metrics for incidents on the network that they control.

Incident: a security event which requires action from the internal security team. This does not include alerts or false positives which can be quickly ruled out.

Steering Committee

The purpose of the steering committee will be to initially define the incident categories, perform web searches for similar systems and to oversee changes. Initially the SC will meet as and when necessary, until version 1 of the 'standard definitions for incident categories' document has been agreed. After this time, it is proposed that they meet quarterly to assess any changes to the categories or their definitions.

At the time of writing, the SC comprises of;

Patrick Green – University of St Andrews (UK)

Jordan M. Schroeder - UCSS InfoSec

Changes to the categories

It is envisaged that there will be changes and enhancements to the categories, entities that feel they need to expand the categories should submit a 'request for enhancement' email, which will be assessed by the SC for approval.

It is not envisaged that the definitions of the categories will change, as this will have a knock on effect for the previous reporting period. If enhancements are made, the SC feels that these are best incorporated with new categories.

Data Collection

At this point, no method has been defined for collecting the metrics from participating entities. It is envisaged that this will be an anonymous process, taking into account the size of the population the reporting entity has. This is detailed below.

Normalisation metric

Once the data has been collected (usually on the last or first day of the month) they will be normalised. This is a standard measure that each entity will provide, so that categories can be measured across entities. The measure used is 'population' – in the case of academic institutes, this means,

Staff+students = population

Metric = population (rounded to nearest 1000)/100

This will then give a figure by which the number of incidents can be divided by, and measured in terms of 'per 100'.

Outputs

It is envisaged that those entities that use the standard categories and submit their metrics in the usual way will be given access to the graphs that are produced. This allows comparisons to be made across entities. Data will be anonymised, and each entity will be given an identifier. For academic institutions, this will be in the form;

U[number]

Sharing Agreement

Graphs and anonymised, normalised data may be shared with external researchers and other relevant parties in the area of network security. Entity names or anything else likely to identify contributors will not be shared.

Anyone who is contributing data may propose additional external entities with whom data should be shared. Proposals should be made via the steering committee who will periodically (as appropriate) circulate the list of current and proposed entities. If no objections are received within 3 weeks of circulating proposed entities data will be shared with those entities.

Current entities with which data is shared:

RUGIT
JANET CSIRT
FIRST / TF-CSIRT
NCSC

Appendix 1

Background reading

IODEF:

http://www.terena.org/activities/tf-csirt/iodef/index.html

NIST:
http://cisecurity.org/en-us/?route=downloads.browse.category.metrics
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

CIS:
http://cisecurity.org/en-us/?route=downloads.browse.category.metrics

US-CERT:
https://www.us-cert.gov/government-users/reporting-requirements