



Document type: Reference

Example Filtered Warning Service Categories

(V1.0) October 2006

Keywords

[Filtered Warnings]

Version control

This document may be made available in more than one electronic version or in print. In a case of existing or perceived difference in contents between such versions, the reference version is the version available for download from the WARP Toolbox site <http://www.warp.gov.uk>

If you find errors in the current document, please send your comment to editor@warp.gov.uk

Disclaimer

Reference to any specific commercial product, process or service by trade name, trademark manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favouring by NISCC. The views and opinions of authors expressed within this document shall not be used for advertising or product endorsement purposes. NISCC shall also accept no responsibility for any errors or omissions contained within this document. In particular, NISCC shall not be liable for any loss or damage whatsoever, arising from the usage of information contained in this document.

Copyright notification

The copyright and the foregoing restrictions, extend to reproduction in all media. The rights to modify and reproduce are described in the WARP Toolbox terms and conditions described on the WARP Toolbox site.

Contents

1	Scope	2
2	Definitions and abbreviations	2
2.1	Abbreviations.....	2
3	Background	2
4	Subscription Categories	2
4.1	High level headings	2
4.1.1	Good practice.....	3
4.1.2	Incident/Threat.....	4
4.1.3	Vulnerabilities/fixes.....	5
5	Conclusions	8
	History	8

1 Scope

This document describes an example set of categories that could be used by a WARP Filtered Warnings Service. Whilst the categories described could be used by a new WARP, the intention is that each WARP will choose their own category structure in order to provide effective filtering of security information.

2 Definitions and abbreviations

2.1 Abbreviations

For the purposes of this document, the following abbreviations apply:

FWA :	Filtered Warnings Application
WARP:	Warning, Advice and Reporting Point

3 Background

The Filtered Warnings Service provides most of its value to WARP members by allowing them to choose the types of security information they wish to receive. The WARP operator will categorise information received from all sources before distribution. The categories chosen by each WARP are therefore very important. This document describes an example set of categories that has been used to construct the default subscription tree provided with the Filtered Warnings Application (FWA), but the same categories could be used by a WARP that does not use FWA.

Each WARP must choose a set of categories for their Filtered Warnings Service that suits their own needs, there is no requirement for a WARP to adopt the specific categories described in this document.

4 Subscription Categories

In the following sections FWA screenshots have been used to illustrate the Subscription Categories - this is just for ease of illustration; there is no requirement to use the FWA when deploying a Filtered Warnings Service.

4.1 High level headings

The example categories described in this document are structured as in a tree style. At the highest level there are three categories:

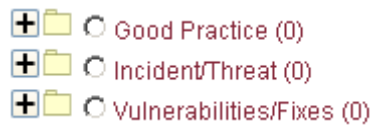


Figure 1 High level categories

The “Good Practice” category is intended to facilitate the distribution of information obtained via the Advice Brokering service.

The “Incident/threat” category is intended to distribute general threat information, and specific information obtained via the Trusted Sharing service.

The “Vulnerabilities/Fixes” category is used to categorise product based security alerts.

4.1.1 Good practice

Within the Good Practice category, sub-categories are used to provide a breakdown of specific interest areas. This example contains a very wide selection of categories. In practice a WARP may have little requirement for such granularity.

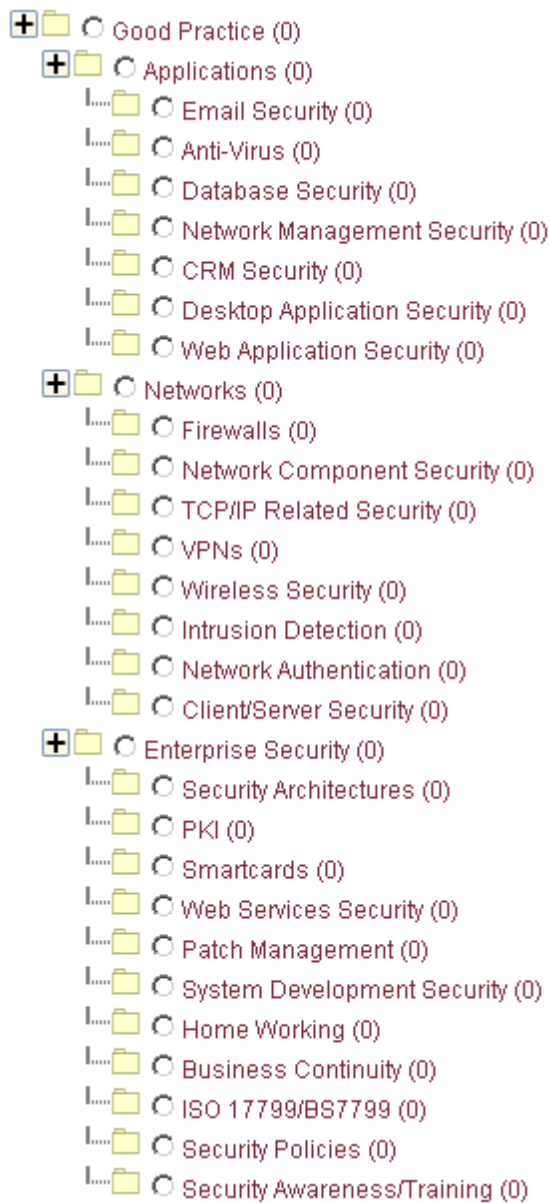


Figure 2 Good Practice Categories

4.1.2 Incident/Threat

The Incident/threat high-level category is split in a similar way to the Good Practice category. Again this level of granularity may not be required. The Filtered Warnings Application makes managing a large number of categories easier, but WARPs not using FWA will probably wish to keep the number of categories offered lower.

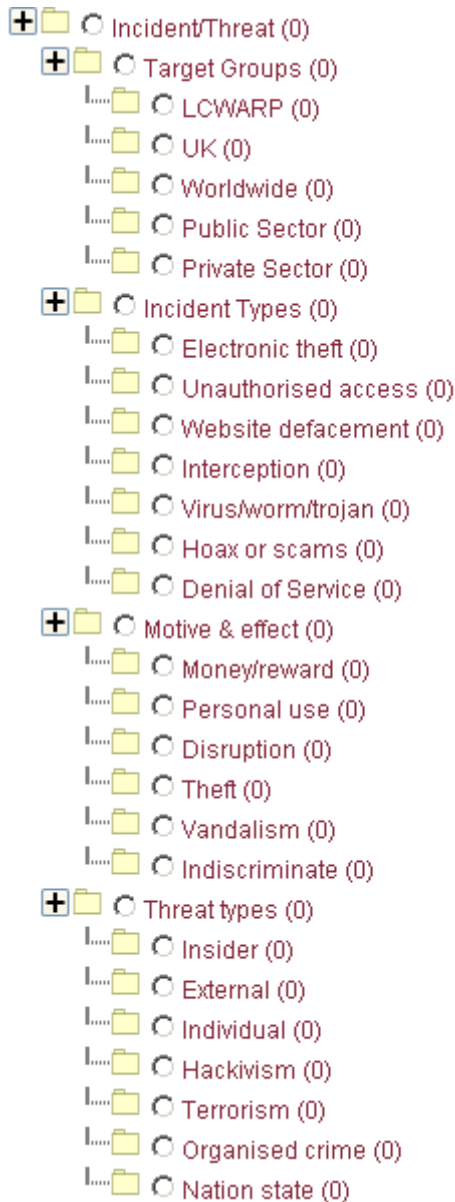


Figure 3 Incident/threat Categories

4.1.3 Vulnerabilities/fixes

The sub-categories in this section are structured around a vendor approach. It may be that a WARP member will be interested in all “Microsoft” and “Sun” security alerts. Alternatively the WARP member may only be interested in certain aspects of a vendor’s product line. The vendor categories in the example are as follows:

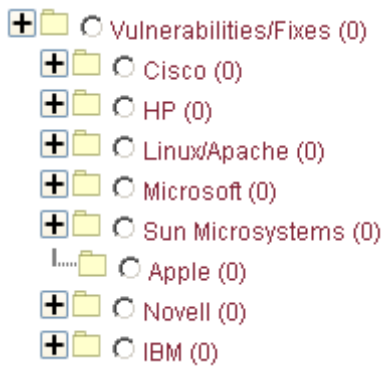


Figure 4 Vendor Categories

Beneath each vendor category, sub-categories have been chosen that attempt to logically divide a particular vendor's product range. This is not necessarily a consistent exercise, depending upon how extensive a vendor's range is. The following images show the categories available for each vendor category. This sub-division may not be required by many WARPs.



Figure 5 Cisco categories

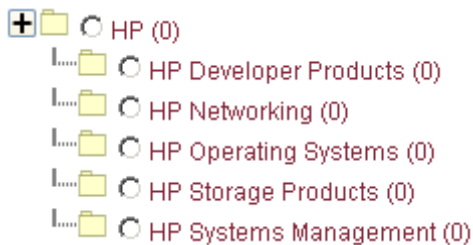


Figure 6 HP categories

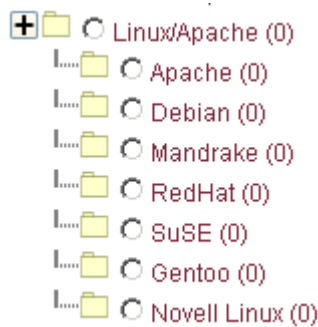


Figure 7 Linux/Apache categories - not a vendor as such; more an open source grouping

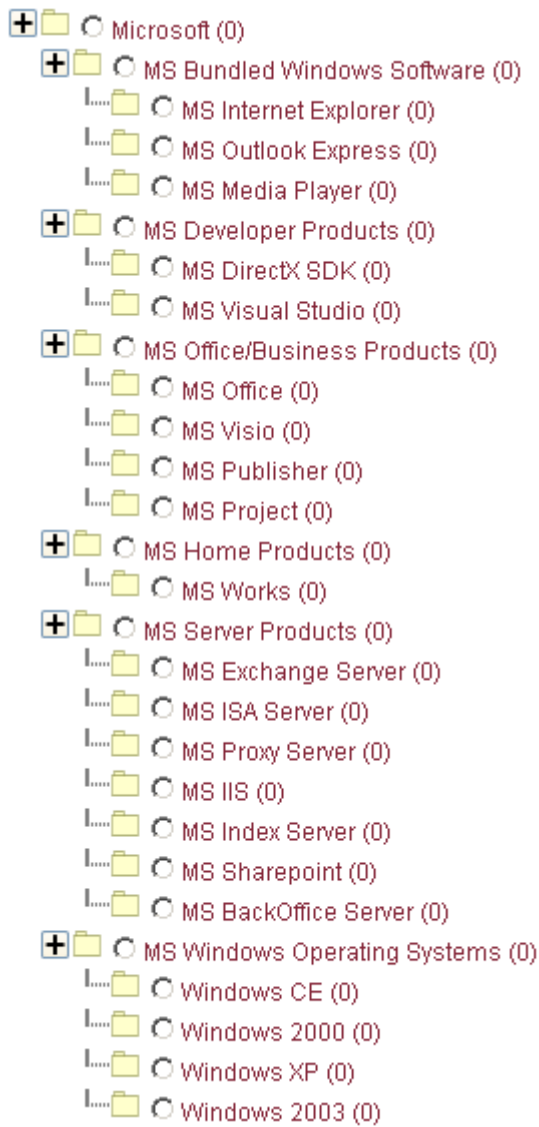


Figure 8 Microsoft categories



Figure 9 Sun categories

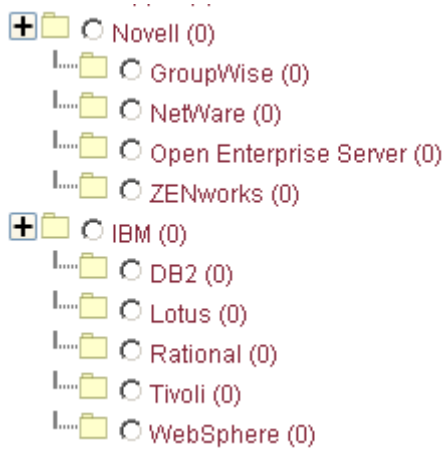


Figure 10 Novell and IBM categories

5 Conclusions

This document shows a very detailed example of categorisation, which was based on some extensive research performed at the beginning of the WARP project. It is important that each WARP reviews the categories used within their Filtered Warnings Service, and creates a structure that provides the most benefit to their members.

History

Version	Date	Description
V1.0	October 2006	Created based on the example FWA tree.