



Toolbox type: Example

(Removable front sheet)

Service definition for a WARP Filtered Warnings Service

(V2.0) July 2006

Keywords

[WARP, Filtered, Warnings, Service Definition]

Important notice

This document is an example of a service definition for the Filtered Warning Service which can be offered by a WARP. It can be used by a WARP Provider to inform their members of the service provided or it can form the basis of a service level agreement. The content can either be provided in paper form, or published in html on the WARPs website.

It is recommended that this example document be edited to produce one which best meets the emerging WARP's specific needs and to which their particular community naming/branding may be applied. This front sheet should therefore be removed and should not form any part of the final document. The WARP Toolbox logo on the next page should be replaced with that of the new WARP if that page is required.

The format of this document is consistent with the WARP Toolbox series of MS Word document templates, which are available as downloads from the WARP Toolbox site.

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.

<Title>

Version: V<x.x>
Date: <Mth yyyy>
Author: <Author>

You can replace this logo with your own if you wish to use this page



Contents

1	Scope	2
2	Definitions	2
3	Description	2
4	Operation	2
4.1	Information sources	2
4.2	Analysis	3
4.3	Tick-list categories.....	3
4.4	Filtering.....	3
4.5	Security	3
4.6	Membership	3
4.6.1	Registration.....	3
4.6.2	Term and charges.....	3
	Appendix: Information sources	4
	History	5

1 Scope

This document provides a high level description of the <insert WARP name> Filtered Warnings Service in order to set the member expectations of the service. Commonly called a Service Definition, it describes important characteristics of the service including resources deployed, costs, security and the information sources analysed.

2 Definitions

For the purposes of this document, the following terms and definitions apply:

- Warnings: A message of this type encourages the recipient to act upon the data contained within it. It supplies information on a very real threat requiring immediate attention and members would be unwise to ignore it.
- Advisories A message of this type provides the recipient with data on a current vulnerability and may include details on security patches. The object of an Advisory is to raise the awareness of a particular security issue.
- Good Practice A message of this type provides information on good practice security measures across a wide range of subjects.

3 Description

Operated and managed by <insert WARP name>, this service will provide the <insert community name> community with the provision of a 'Filtered Warnings Service'. The basic concept is that <insert WARP name> members will define their subscription profile by completing an on-line 'secure' tick-list that identifies their area of interest. Warnings and Advisories from a number of sources, including UNIRAS and the <insert WARP name> itself, will be filtered against the tick-list criteria for relevance and urgency and disseminated via authenticated email in a timely manner. This filtering will be carried out using the Filtered Warnings Application software.

4 Operation

4.1 Information sources

The primary sources of information used to generate the Warnings and Advisories sent via this service can be found in the Appendix - Information Sources.

4.2 Analysis

These information sources will be analysed every working day and it is estimated that 30% to 40% of the time will be spent carrying out this analysis. An average performance target from receiving information from one of the sources, analysing the information and sending out the filtered resulting emails, is 2 hours turn round in normal working hours. At other times reasonable endeavours applies.

4.3 Tick-list categories

The three high level categories for members to choose from are: Vulnerabilities & fixes, Incidents & threats, and Good Practice. The sub-categories are chosen to meet the needs of the community and can be viewed by logging onto the Filtered Warnings Application located within the <insert WARP name> website at <insert WARP website url>.

4.4 Filtering

<Insert WARP Name> will provide this service by using a secure on-line tick-list to determine the type of information members require. Based on this data, specific information sources can be targeted and the Warnings and Advisories that are generated via the Filtered Warnings Application software can be sent to the correct people.

4.5 Security

Members must be assured that any Warning or Advisories that they receive are originating from the <insert WARP name>. Using authenticated emails through the Filtered Warnings Application will facilitate this.

4.6 Membership

4.6.1 Registration

In order for members to receive filtered warnings, advisories and good practice news from the <insert WARP name>, they may wish to set up a dedicated WARP email address e.g. warp@domain.name. Alternatively they could use their existing email address. To register for the Filtered Warnings Service, <insert WARP name> members will need to obtain a username and password from their <insert WARP name> Provider. The <insert WARP name> member should then logon to the service at <insert WARP website url>, enter their email address and set up their subscription profile using the on-line tick list.

4.6.2 Term and charges

Membership lasts for a year and is free for the year 2004/05. It is intended that a small subscription be charged for membership for subsequent years. The level of this is yet to be determined and will be dependant on vendor sponsorship as well as the number of members signed up. <amend section as appropriate>

Appendix: Information sources

UNIRAS	the UK government's CERT and fully integrated part of NISCC. It responds to electronic attack and issues Warnings and Alerts regarding IT security incidents and vulnerabilities. URL – http://www.uniras.gov.uk/
Microsoft	useful security resource for IT professionals, home and business users alike along with security bulletins and patches for Microsoft products. Also provides some information on some current viruses. URL http://www.microsoft.com/security/ Mailing list - http://www.microsoft.com/technet/security/bulletin/notify.msp
Zone H	tracks hacking attacks and defacements on websites all over the world. Includes attack statistics along with the latest news and advisories on cyber security. URL – http://zone-h.org
Symantec	a world leader in Internet security technology, provides a broad range of content and network security software and appliance solutions to individuals, enterprises and service providers. They provide excellent virus information along with very useful statistics. URL http://securityresponse.symantec.com Mailing list - http://nct.symantecstore.com/virusalert/
Sophos	a world leader in anti-virus protection, focused on defending businesses of all sizes from virus attack. They are a good source of information on the latest viruses along with news of current InfoSec issues. URL – http://www.sophos.com Mailing list - http://www.sophos.com/security/notifications
MessageLabs	provides intelligence on a range of information on global email security threats. The service has live data feeds from their control towers around the world, which scan millions of emails everyday, and therefore provide the latest and most comprehensive data and analysis available. URL – http://www.messagelabs.com/Threat_Watch Mailing list - Subscription available on the same page.
Cisco Systems	URL http://www.cisco.com/security/ Mailing list - http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html#subscribe
Sun Microsystems	URL http://sunsolve.sun.com/ Mailing list - http://sunsolve.sun.com/pub-cgi/show.pl?target=security/sec
Silicon Graphics, Inc.	security advisories and patches for SGI's range of software products. URL – http://www.sgi.com/support/security/ Mailing list - http://www.sgi.com/support/security/wiretap.html

Apache Software The Apache Software Foundation provides support for the Apache community of open-source software projects. The Apache projects are characterized by a collaborative, consensus based development process, an open and pragmatic software license, and a desire to create high quality software that leads the way in its field. URL - <http://www.apache.org/>

HP Software Hewlett Packard's software division URL - <http://www.software.hp.com/>

History

Version	Date	Description
V1.0	June 2004	First issue
V1.1	July 2004	Updated template
V2.0	July 2006	Updated links