ETSI GS ISI 001-2 V1.1.1 (2013-04)

Information Security Indicators (ISI); Indicators (INC); Part 2: Guide to select operational indicators based on the full set given in part 1

Disclaimer

This document has been produced and approved by the Information Security Indicators (ISI) ETSI Industry Specification Group (ISG) and represents the views of those members who participated in this ISG.
It does not necessarily represent the views of the entire ETSI membership.

Reference
DGS/ISI-001-2

Keywords
ICT, security

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

Individual copies of the present document can be downloaded from:
 http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, please send your comment to one of the following services: http://portal.etsi.org/chaircor/ETSI_support.asp

Copyright Notification

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://ipr.etsi.org).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Group Specification (GS) has been produced by ETSI Industry Specification Group (ISG) Information Security Indicators (ISI).

The present document is part 2 of a multi-part deliverable covering the Information Security Indicators (ISI); Indicators (INC), as identified below:

Part 1: "A full set of operational indicators for organizations to use to benchmark their security posture";

Part 2: "Guide to select operational indicators based on the full set given in part 1".

The present document is included in a series of 6 ISI 00x specifications. These 6 specifications are the following (see figure 1 summarizing the various concepts involved in event detection and interactions between all specifications):

- The present document addressing (together with its base list of indicators described in GS ISI 001-1 [5]) information security indicators, which are meant to measure application and effectiveness of preventative measures.
- GS ISI 002 addressing the underlying event classification model and the associated taxonomy.
- GS ISI 003 addressing the key issue of assessing organization's maturity level regarding overall event detection (technology/process/ people) and to weigh event detection results.
- GS ISI 004 addressing demonstration through examples how to produce indicators and how to detect the related events with various means and methods (with a classification of the main categories of use cases/symptoms).
- GS ISI 005 addressing ways to produce security events and to test the effectiveness of existing detection means within organization (for major types of events), which is a more detailed and a more case by case approach than ISI 003 one and which can therefore complement it.