ETSI GS ISI 003 V1.1.2 (2014-06)

Information Security Indicators (ISI); Key Performance Security Indicators (KPSI) to evaluate the maturity of security event detection

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
RGS/ISI-006

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

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

GS ISI 001-1 [1]: addressing (together with its associated guide GS ISI 001-2 [2]) information security indicators, meant to measure application and effectiveness of preventative measures.

GS ISI 002 [3]: addressing the underlying event classification model and the associated taxonomy.

GS ISI 003: addressing the key issue of assessing an organisation's maturity level regarding overall event detection (technology/process/ people) and to evaluate event detection results.

GS ISI 004 [4]: 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 [i.1]: addressing ways to produce security events and to test the effectiveness of existing detection means within an organization. More detailed and more a case by case approach than the present document and therefore complementary.

Figure 1 summarizes the various concepts involved in event detection and the interactions between the specifications.

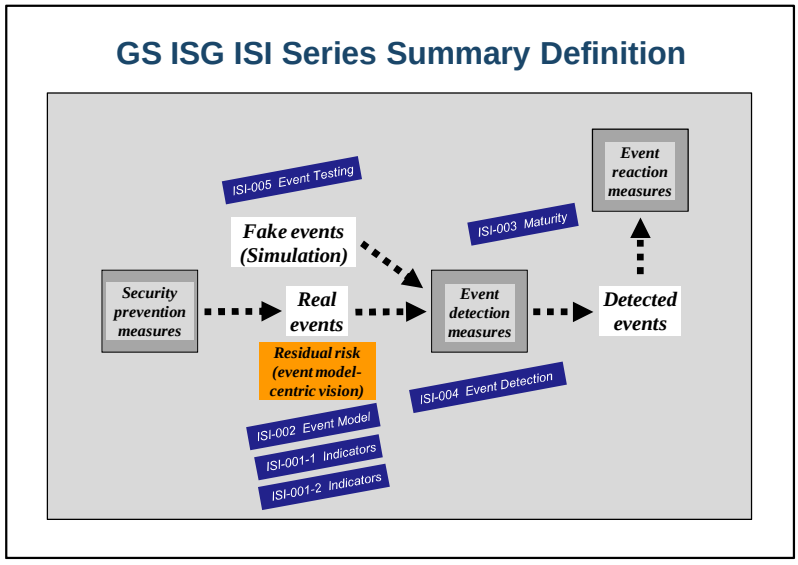

Figure 1: Positioning the 6 GS ISI against the 3 main security measures

Introduction

The present document addresses the event detection aspects of the information security processes in an organization. The maturity level assessed during event detection can be considered as a good approximation of the overall Cyber Defence and SIEM maturity level of an organization.

1 Scope

The present document defines and describes a set of Key Performance Security Indicators (KPSI) to be used for the evaluation of the performance, the maturity levels of the detection tools and processes used within organizations for security assurance. The response is not included in the scope of the present document.

In particular, the purpose of the present document is to enable organizations to:

- assess the overall maturity level of the security event detection;
- provide a reckoning formula to assess detection levels of major security events as summarized in GS ISI 001-1 [1];
- evaluate the results of measurements.

This work is mainly based on the US SANS CAG [5].

The target groups of the present document are Head of detection, reaction teams, Cyber defence team and head of security governance.

2 References

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

2.1 Normative references

[1] ETSI GS ISI 001-1: "Information Security Indicators (ISI); Indicators (INC); Part 1: A full set of operational indicators for organizations to use to benchmark their security posture".

[2] ETSI GS ISI 001-2: "Information Security Indicators (ISI); Indicators (INC); Part 2: Guide to select operational indicators based on the full set given in part 1".

[3] ETSI GS ISI 002: "Information Security Indicators (ISI); Event Model A security event classification model and taxonomy".

[4] ETSI GS ISI 004: "Information Security Indicators (ISI); Guidelines for event detection implementation".

[5] SANS Consensus Audit Guidelines V4.0: "20 Critical Security Controls for Effective Cyber Defence".

[6] The Capability Maturity Model Integration (Software Engineering Institute, 2001).

[7] Portfolio, Programme and Project Management Maturity Model (OGC, 2008).

NOTE: See http://www.sans.org/critical-security-controls/ for an up-to-date version.