ETSI GS ISI 002 V1.2.1 (2015-11)

Information Security Indicators (ISI);
Event Model
A security event classification model and taxonomy

Reference
RGS/ISI-002ed2

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 parts):

- ETSI GS ISI 001-1 [i.3] addressing (together with its associated guide ETSI GS ISI 001-2 [i.4]) information security indicators, meant to measure application and effectiveness of preventative measures.
- The present document (ETSI GS ISI 002) addressing the underlying event classification model and the associated taxonomy.
- ETSI GS ISI 003 [i.11] addressing the key issue of assessing an organization's maturity level regarding overall event detection (technology/process/ people) in order to evaluate event detection results.
- ETSI GS ISI 004 [i.12] 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).
- ETSI GS ISI 005 [i.13] addressing ways to produce security events and to test the effectiveness of existing detection means within organizations (for major types of events), which is a more detailed and a more case by case approach than in ETSI GS ISI 003 [i.11] and which can therefore complement it.

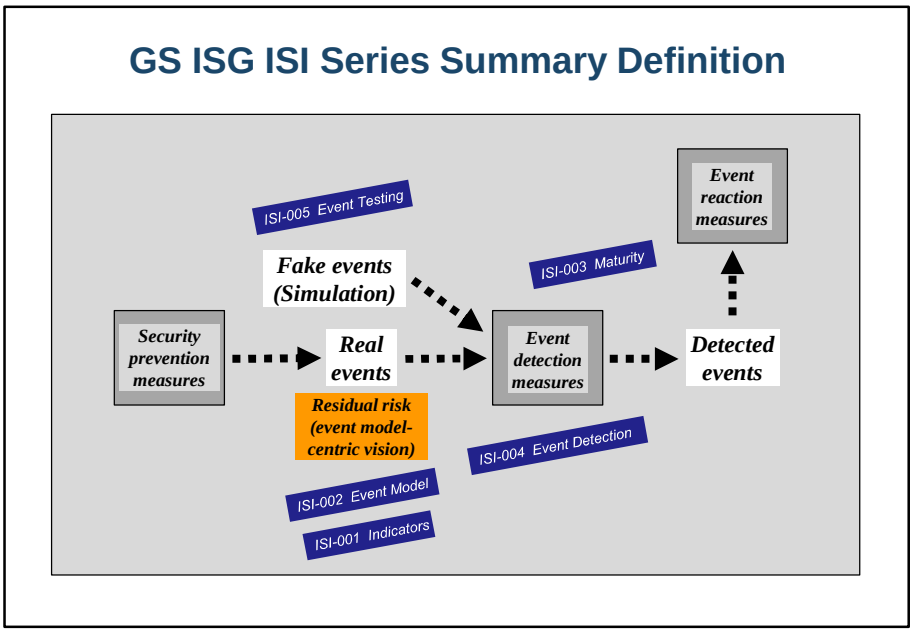

Figure 1: Positioning the 5 GS ISI against the 3 main security measures

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Introduction

A corporate Cyber Defence and SIEM approach implements continuously security improvements with the main goals to:

- operationally and constantly reduce the **residual risk** incurred by their Information Systems (see figure 2, which highlights the two associated types of events - incidents and vulnerabilities - and the joint area covered by IT security policy through the concept of usage or implementation drift); and
- to assess the actual **application** and real **effectiveness** of their **security policies** (or of their ISMS, if they have one), for the purpose of their constant improvement.

Such an approach, which to a large extent relies on using the traces available in the Information System's various components, is organized around an **"event-model centric"** vision, and can also be tied up to the PDCA model that is commonly used in quality and security areas. As such, this primarily involves implementing this model's PDCA "Check" step on the basis of very detailed knowledge of threats and vulnerabilities.

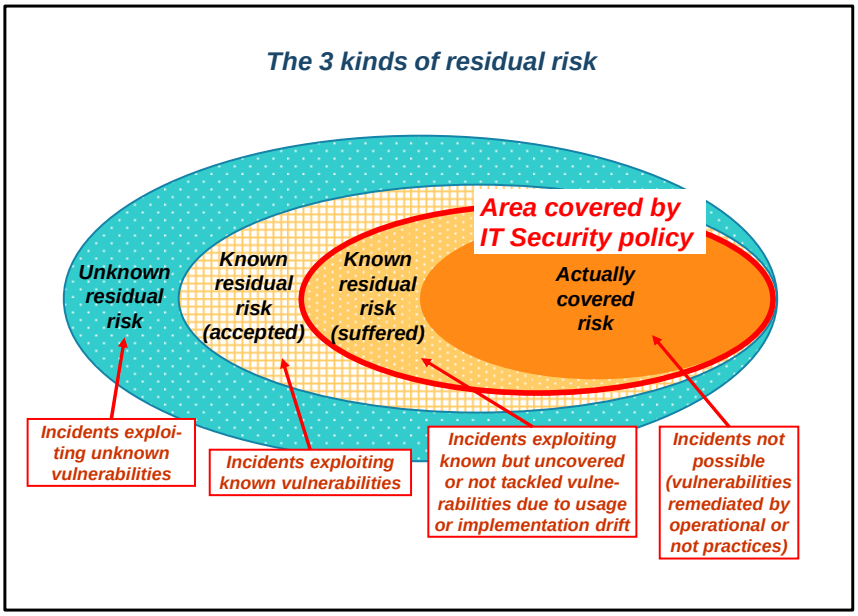

Figure 2: The 3 kinds of residual risks

Worldwide trends in ICT security show that significant progress can be accomplished within a few years with the deployment of an organization-wide operational Cyber Defence and SIEM approach. A recent survey by a major consulting firm of 15 major companies and organizations brings to light nine key success criteria. The two most important criteria are:

- The reliance of the Cyber Defence and SIEM approach on a security event classification model that takes into account both incidents and vulnerabilities, and that stresses particular attention to malicious and intentional acts, the monitored events themselves being selected on the basis of main relevant CIA risks and associated metrics (e.g. statistics).
- Training with this model for the relevant people using the Information System, with particular attention to the presentation of concrete examples of disasters associated with inventoried security event main types.

As such, the present document's objective is to build a **full taxonomy** to thoroughly describe all IT security events (and when appropriate and necessary non-IT security events) and, based on this, to present an **original representation** that leverages the current international best practices and enables diversified and complex uses. The choice of a detailed taxonomy, which describes security events through a set of attributes (different for incidents and vulnerabilities), ensures that all possible situations can be taken into account with the required flexibility (especially thanks to the provided open dictionary), while the representation chosen for the taxonomy, highlighting the main categories generally accepted by industry consensus, makes the event classification model easier to understand and embrace for stakeholders.

The present document is based on work carried out by the Club R2GS®, a French association created in 2008, specializing in Cyber Defence and Security Information and Event Management (SIEM), gathering large French companies and organizations (mainly users). The present document (ETSI GS ISI 002), as well as the other GS of ISG ISI, are therefore **based on a strong experience**, this community of users having adopted and used the event classification model and the related reference framework for indicators for more than three years on a national and world-wide scale.

1 Scope

The present document provides a comprehensive security event classification model and associated taxonomy (based on existing results and hands-on user experience), covering both security incidents and vulnerabilities. The two latter ones become nonconformities when they violate an organization's security policy. The present document mainly supports operational security staff in their effort to qualify and categorize detected security events, and more generally all stakeholders (especially CISOs and IT security managers) in their needs to establish a common language.

2 References

2.1 Normative 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 reference 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.

The following referenced documents are necessary for the application of the present document.

Not applicable.

2.2 Informative 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 reference document (including any amendments) applies.

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

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] NIST SP 800-126 Revision 2 (September 2011): "The Technical Specification for the Security Content Automation Protocol (SCAP): SCAP Version 1.2".

[i.2] MITRE CCE List Version 5.20120314 (March 2012): "Common Configuration Enumeration".

[i.3] 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".

[i.4] 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".

[i.5] ISO/IEC 27000:2012: "Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary".

[i.6] draft-ietf-mile-rfc5070-bis-11: "The Incident Object Description Exchange Format v2".

[i.7] ISO 27002:2013: "Information technology -- Security techniques -- Code of practice for information security management".

[i.8] ISO 27004:2009: "Information technology -- Security techniques -- Information security management -- Measurement".

[i.9] ISO 27005:2011: "Information technology -- Security techniques -- Information security risk management".