ETSI GS ISI 002 V1.1.1 (2013-04)

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

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-002

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 5
Foreword 5
Introduction 6
1 Scope 8
2 References 8
2.1 Normative references 8
2.2 Informative references 8
3 Definitions and abbreviations 9
3.1 Definitions 9
3.2 Abbreviations 13
4 Positioning of the proposed event classification model 15
4.1 Relationship with the ISO 27004 standard 15
4.2 The critical importance of positioning the model appropriately 15
4.3 The necessity for the model to rest on a detailed taxonomy 17
4.4 Description of the taxonomy 17
4.5 Complex security incidents versus basic security incidents 19
4.6 The key drivers underlying the representation proposed 20
4.7 The general description of the representation 20
4.8 Link between the event model representation and the list of indicators (and related families) 21
5 Comparison with other event classification models 21
5.1 Risk analysis methods classifications 22
5.2 CAPEC classification 22
5.3 FIRST classifications 23
6 Detailed description of the proposed representation of the different categories and sub-categories 23
6.1 Intrusions and external attacks (Category IEX) 23
6.2 Malfunctions (Category IMF) 25
6.3 Deviant internal behaviours (Category IDB) 27
6.4 Behavioural vulnerabilities (Category VBH) 29
6.5 Software vulnerabilities (Category VSW) 31
6.6 Configuration vulnerabilities (Category VCF) 32
6.7 General security (technical & organizational) vulnerabilities (Category VTC and Category VOR) 33
7 Practical uses of the event classification model 34
7.1 The classification model pivotal role 35
7.2 The objective shared with operational risks 36
7.3 The link with existing studies on cybercrime motivation (threat intelligence) 36
7.4 Other uses of the classification model 39
Annex A (informative): Overview of the ISO 27004 standard measurement model 41
Annex B (informative): Field dictionary for the taxonomy 42
B.1 Incidents 42
B.1.1 Who and/or Why 42
B.1.1.1 Accident 42
B.1.1.2 Unwitting or unintentional act (error) 42
B.1.1.3 Unawareness or carelessness or irresponsibility 43
B.1.1.4 Malicious act 43
B.1.2 What 44
B.1.2.1 Unauthorized access to a system and/or to information 44
B.1.2.2 Unauthorized action on the information system and/or against the organization 45
B.1.2.3 Installation of unauthorized software programs (malware) on a system (without the owner's consent) 46
B.1.2.4 Information system remote disturbance 46
B.1.2.5 Social engineering attacks 46
B.1.2.6 Personal attack on organization's personnel or organization disturbance 47

B.1.2.7 Physical intrusion or illicit action 47
B.1.2.8 Illicit activity carried out on the public Internet (harming an organization) 47
B.1.2.9 Various errors (administration, handling, programming, general use) 48
B.1.2.10 Breakdown or malfunction 49
B.1.2.11 Environmental events (unavailability caused by a natural disaster) 49
B.1.3 How 49
B.1.3.1 Unauthorized access to a system and/or to information 49
B.1.3.2 Unauthorized action on the information system and/or against the organization 50
B.1.3.3 Installation of unauthorized software programs (malware) on a system (without the owner's consent) 52
B.1.3.4 Information system remote disturbance 52
B.1.3.5 Social engineering attacks 53
B.1.3.6 Personal attack on organization's personnel or organization disturbance 53
B.1.3.7 Physical intrusion or illicit action 53
B.1.3.8 Illicit activity carried out on the public Internet network (harming an organization) 54
B.1.3.9 Various errors (administration, handling, programming, general use) 54
B.1.3.10 Breakdown or malfunction 54
B.1.3.11 Environmental events (unavailability caused by a natural disaster) 54
B.1.4 Status 55
B.1.4.1 Security event attempt (or occurrence) underway 55
B.1.4.2 Succeeded (or performed) security event 55
B.1.4.3 Failed security event 55
B.1.5 With what vulnerability(ies) exploited (up to 3 combined kinds of vulnerabilities) 55
B.1.5.1 Behavioural vulnerability 55
B.1.5.2 Software vulnerability 55
B.1.5.3 Configuration vulnerability 55
B.1.5.4 General security vulnerability 55
B.1.5.5 Conception vulnerability 55
B.1.5.6 Material vulnerability 55
B.1.6 On what kind of asset 56
B.1.6.1 Data bases and applications 56
B.1.6.2 Systems 56
B.1.6.3 Networks and telecommunications 58
B.1.6.4 Offline storage devices 59
B.1.6.5 End-user devices 59
B.1.6.6 People 60
B.1.6.7 Facilities and environment 61
B.1.7 With what CIA consequences 61
B.1.7.1 Loss of confidentiality (with types of loss and with the amount of data as a possible complement) 61
B.1.7.2 Loss of integrity (with types of loss) 63
B.1.7.3 Loss of availability (with types of loss and with the duration as a possible complement) 63
B.1.8 With what kind of impact 63
B.1.8.1 Direct impact 63
B.1.8.2 Indirect impact 64
B.2 Vulnerabilities 64
B.2.1 What 64
B.2.1.1 Behavioural vulnerabilities 64
B.2.1.2 Software vulnerabilities 67
B.2.1.3 Configuration vulnerabilities 67
B.2.1.4 General security (organizational) vulnerabilities 68
B.2.1.5 Conception vulnerability 70
B.2.1.6 Material vulnerability 70
B.2.2 On what kind of assets 71
B.2.3 Who (only for behavioural vulnerabilities) 71
B.2.4 For what purpose (only for behavioural vulnerabilities) 71
B.2.5 To what kind of possible exploitation 71
Annex C (informative): Authors & contributors 72
Annex D (informative): Bibliography 73
History 75

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 00x specifications. These 6 specifications are the following (see figure 1 summarizing the various concepts involved in event detection and interactions between all parts):

- GS ISI 001-1 [3] addressing (together with its associated guide GS ISI 001-2 [4]) information security indicators, meant to measure application and effectiveness of preventative measures.
- The present document (GS ISI 002) addressing the underlying event classification model and the associated taxonomy.
- GS ISI 003 [i.5] addressing the key issue of assessing organization's maturity level regarding overall event detection (technology/process/ people) in order to weigh event detection results.
- GS ISI 004 [i.6] 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.7] 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 GS ISI 003 one [i.5] and which can therefore complement it.

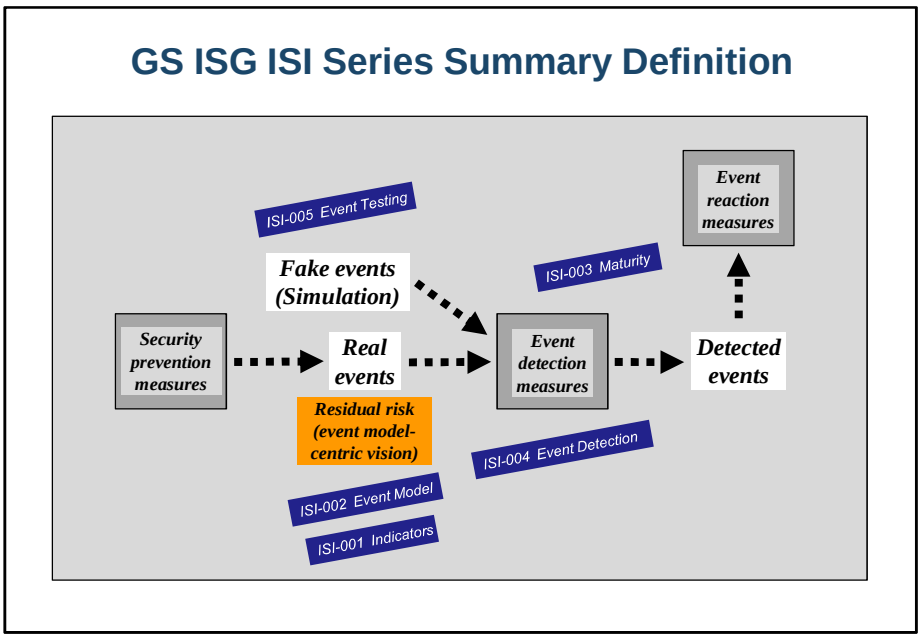

Figure 1: Positioning the 5 GS ISI 00x against the 3 main security measures

Introduction

An overall corporate Cyber Defence and SIEM approach is intended to implement continuous security improvement within large organizations, with the main following goals:

- operationally and constantly reduce the **residual risk** incurred by their Information Systems (see chart below, which highlights the 2 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 necessarily 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.

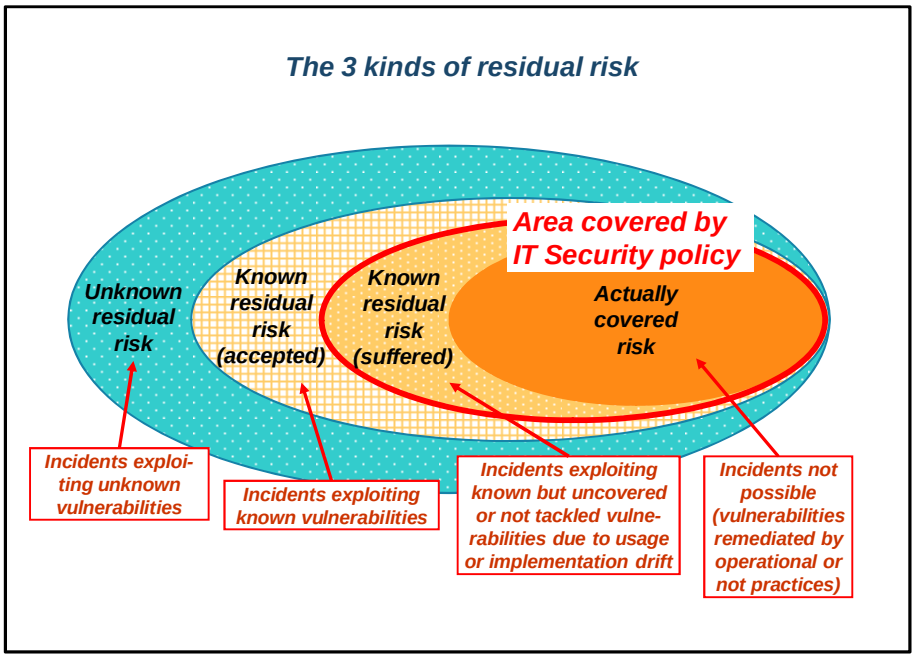

Figure 2: The 3 kinds of residual risks

The recent 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 approach and SIEM approach. Also, a recent survey by a major consulting firm of 15 major companies and organizations brings to light 9 key success criteria. It is worth mentioning the two most important criteria:

- 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 notably 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 it, 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. And this representation is key because acceptance by all will depend mainly on it.

It should be finally mentioned that the present document rests in part on work carried out by Club R2GS (see Annex D – Bibliography), a French association created by the end of 2008, specializing in Cyber Defence and Security Information and Event Management (SIEM) and gathering most very large companies and organizations (mainly users) amongst the most advanced ones in France regarding these topics. The present document (GS ISI 002), as well as all other GS ISI 00x, is 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 sometimes over 3 years, and in some cases on a world-wide scale.