ETSI GS ISI 004 V1.1.1 (2013-12)

Information Security Indicators (ISI); Guidelines for event detection implementation

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-004

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

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 multi-part 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 addressing (together with its companion guide GS ISI 001-2) information security indicators, 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 organisation'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.

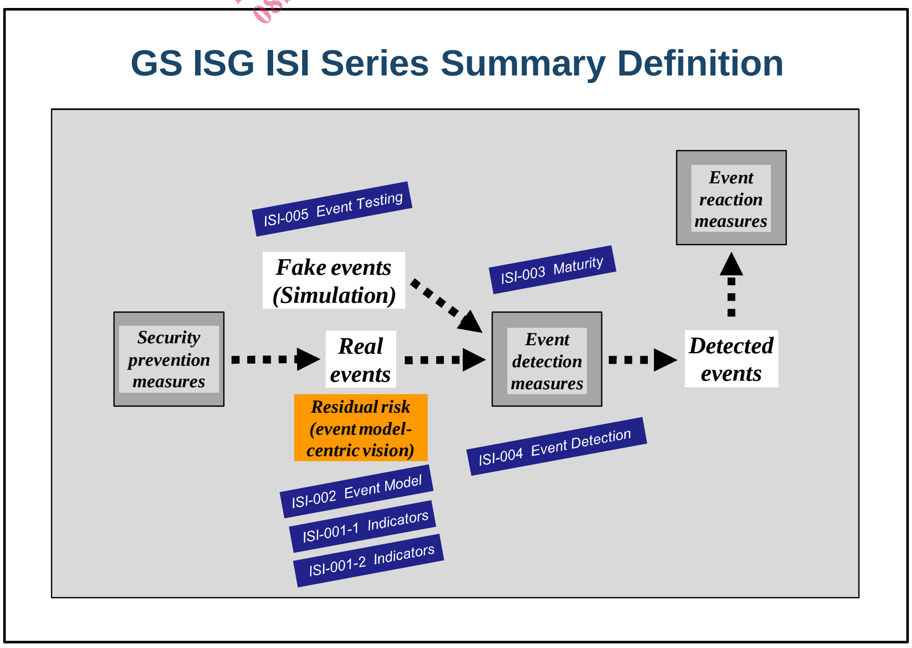

Figure 1: Positioning the 6 GS ISI multi-parts against the 3 main security measures

Introduction

The purpose of the present document, which is the engineering part of the ISG ISI 5-part series, is to:

- present a comprehensive classification of the main symptoms/use cases (in some cases also referred to as indicators of compromise) to look for in IT system traces in order to detect stealthy events (as listed in GS ISI 002 [i.3]);
- position all these elements of information within a consistent framework (MITRE CybOX standard) in order to ease their exchange between various security stakeholders (such as CSIRTs, SOCs, administrators, etc.);
- give some examples of frequent security events in order to illustrate powerful means and methods of detection.

The present document addresses only events detected through technical means, and only security incidents and behavioural vulnerabilities, excluding all other kinds of vulnerabilities (software, configuration and general security), since these latter are far simpler to detect with well-identified and well-established methods and tools. And regarding security incidents, focus is stressed mainly on attacks of a malicious nature.

1 Scope

The scope of the present document is to define and describe a classification of the main symptoms/use cases, which are used to detect security events listed in GS ISI 002 [i.3].

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] ISO/IEC 27002:2013: "Information technology -- Security techniques -- Code of practice for information security controls".

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

2.2 Informative references

[i.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".

[i.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".

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

3 Definitions and abbreviations

3.1 Definitions

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

NOTE: See also the summary chart at the end of this list.

asset: entity (information or physical component) that has value to the organization and that can be broken down in primary assets (such as business activities, data, application software, etc. which hold the business value) and secondary/supporting assets (network or system infrastructure, which host primary assets)

assurance: planned and systematic activities implemented in a management system so that management requirements for a service will be fulfilled

NOTE: It is the systematic measurement, comparison with a standard, monitoring of processes and an associated feedback loop that confers error prevention. This can be contrasted with Management "Control", which is focused on process outputs.

base measure: regarding the "indicator" definition, defined in terms of an attribute and the specified measurement mean for quantifying it (e.g. number of trained personnel, number of sites, cumulative cost to date)

NOTE: As data is collected, a value is assigned to a base measure.

continuous auditing: periodic verification and collection of a series of controls identified within the Information System, corresponding to the detection of incidents and of software, configuration, behavioural or global security framework vulnerabilities and/or non-conformities

NOTE: There are three auditing levels (in principle, hierarchy notably implemented within banking and financial institutions):

- Detailed behavioural, global security framework or technical checking at the security software or equipment level (network, system, application software).
- Level 1 auditing via monitoring of trends and deviations of a series of significant measurement points.
- Level 2 auditing (verification of existence of an appropriate level of assurance and technical coverage of the chosen control and measurement points, and of implementation of regulatory requirements).

Continuous auditing can be either manual or automatic (for example, monitoring by means of tools appropriate for a SIEM approach). Finally, continuous auditing is generally associated with statistical indicators (levels of application and effectiveness of security controls), that provide information regarding the coverage and assurance level of the security controls in question.

criticality level (of a security event): level defined according to the criteria which measures its potential impact (financial or legal) on the company assets and information, and which make it possible to evaluate the appropriate level of reaction to the event (incident treatment or vulnerability or nonconformity removal)

NOTE: The criticality level of a given event is determined by the combination of its severity level (inherent to the event itself - see definition below) and of the sensitiveness of the target attacked or concerned (linked to the asset estimated value for the company - whose value concerns confidentiality, integrity or availability). This concept of criticality level (usually defined on a scale of four levels) is at the core of any SIEM approach, for which classifying security events processing according to organization-defined priorities is vital from both a security and economic point of view.

derived measure: regarding the "indicator" definition, measure that is derived as a function of two or more base measures

effectiveness (of security policy or of ISMS): As a supplement to the actual application of security policy (or of ISMS) and of its measures assessment, it is necessary to assess its level of effectiveness, that can be estimated through identified residual risk (that corresponds with the residual vulnerabilities that are actually exploited and that have led to security incidents).

NOTE: It should be added that the term "efficiency" is sometimes also used, but generally with a different meaning of economy in the use of resources (not addressed here for reasons of lesser relevancy).

(security) incident: single unwanted or unexpected security event, or series thereof, that correspond to the exploitation of an existing vulnerability (or attempt to), and with an actual or potential threat (attempt underway), that have a significant probability of compromising business operations and threatening information security

NOTE: In case of success, an incident affects nominal operations of all or part of an information system (according to the Confidentiality, Integrity and Availability criteria - English acronym CIA). An incident that manifests itself through previously unseen phenomena, or is built as a complex combination of elementary incidents often cannot be qualified and therefore inventoried or categorized easily; such an incident will often be referred to as an anomaly.

indicator: measure that provides an estimate or evaluation of specified attributes derived from an analytical model with respect to a defined information need

NOTE: Indicators are the basis for analysis and decision making.

log: continuous recording of computer usage data, with specific characteristics: detailed and specified structure, time-stamping, recording as soon as they occurs in files or other media

NOTE: Logs are a kind of trace (more general concept - see definition below).

non-conformity: security event that indicates that organization's required security rules and regulations have not been properly enforced, and are therefore the consequence of a usage or implementation drift

NOTE: Continuous monitoring of non-conformities (similar to continuous auditing - Cf. this term above) enables to better ensure that an organization's security policy is being enforced. Non-conformity can be further refined according to their kind: configuration, behaviour, global security (technical and organizational) and material. Non-conformities are also vulnerabilities or incidents, depending on the situation (see definition).

periodic audit (Periodic scanning): using isolated audit means, periodic acquisition and verification of security controls

NOTE: A periodic audit can also be either manual or automatic (for example, carried out through scanner type tools). Finally, a periodic audit is generally Boolean (all or nothing compliance level).

risk: product of the probability of occurrence of a security incident involving a specific asset by its impact on this asset (impact assessed according to the CIA sensitivity level)

NOTE: The level of risk exposure (concept which is used in risk assessment methods) corresponds to the product of the vulnerability level of the asset in question by the threat level hanging over it.

risk not covered (by existing security measures): Risk sometimes also referred to as "residual", which breaks down into 3 shares:

- Known and realized suffered risk, corresponding to the impact suffered by the organization under attack when the security policy is not applied (configuration, behavioural or global security non-conformities), and when known and critical software vulnerabilities are not appropriately addressed.
- Known and accepted risk that corresponds to a risk taken by choice by an organization, by comparing the risk associated with attacks with economic, usage and security level considerations.
- Unknown risk associated with unknown and unpatched vulnerabilities, or innovative attack vectors.

security event: information about a change of state in a system that may be security relevant and that indicates the appearance of a risk for the organization

NOTE: A security event is either an incident or a vulnerability occurrence or detection (see definition of these terms). 500 security events have been inventoried within the industry, and are grouped into 7 major categories, with the 3 first corresponding to incidents, and the 4 last to vulnerabilities: external attacks and intrusions, malfunctions, internal deviant behaviours, behavioural vulnerabilities, software vulnerabilities, configuration vulnerabilities, general security (technical or organizational) vulnerabilities.

Security Information and Event Management (SIEM) solutions: combination of the formerly separated product categories of SIM (security information management) and SEM (security event management)

NOTE 1: SEM deals with real-time monitoring, correlation of events, notifications and console views. SIM provides long-term storage, analysis and reporting of log data.

NOTE 2: The present document extends these two notions under the generic SIEM acronym, which encompasses all organizational, processes and human aspects necessary to deploy and operate these tools, and which include vulnerability and nonconformity management; we may refer to Cyber Defence approaches in the most complex case.

security policy: overall intention and requirements as formally expressed by management

NOTE: Two levels are used: general statements and detailed rules. General statements are consistent with controls within ISO/IEC 27002 [1] standard. Rules apply to network and systems configuration, user interaction with systems and applications, and detailed processes and procedures (governance, operational teams, and audit). Violation of a rule brings about nonconformity, which is either an incident or vulnerability.

sensitivity level: level which corresponds to the potential impact (financial, legal or brand image) of a security event on an asset, an impact linked to the estimated value of the asset for the company along four possible viewpoints: its Confidentiality, Integrity and Availability (CIA) and sometimes its accountability

severity level (of security incident): Level (generally defined on a 4-element scale) inherent to the event itself and that depends on several criteria that vary according to the types of events (in decreasing order of importance):

- *Dangerousness* is the result of multiple factors combined together according to circumstances or types of incidents: propagation speed for a worm, virulence, effectiveness, importance and number of impacted assets, capability of harm, target reachability, capability of remote action, persistence, weakness or lack of curative means, and extend of compromise (depth of component which is can be or has been reached, concept of Defence in Depth or DiD).

- *Stealthiness* covers the level to which the incident can be hidden to the defender: obvious visibility, visible through simple and easy to use mechanisms, detection requires advanced technical tools, almost invisibility. It is a key factor for monitoring and detection. Anonymization and camouflage, or active and passive masking techniques are stealthiness techniques. Stealthiness takes on an indirect meaning when it applies to similar not yet detected incidents.

- *Feasibility* describes the attacker's motivation and skills. It increases proportionally to all the necessary prerequisites (regarding skills, tools, financial means, collusion, initial access, etc.) combined with the presence of exploitable vulnerabilities; feasibility can be tied often to the frequency of attacks that can be detected in the world. Its assessment is not simple, because it is subject to change. For example, it may be difficult to create a hacking tool for a given vulnerability. However, once the tool is released on the Internet, it can be used by unskilled attackers. Feasibility takes on an indirect meaning when it applies to a potential threat (see definition of this term), as the analysis of its factors required to evaluate it provides an interesting evaluation of the risk.

NOTE: This notion appeared in the mid-1990s within the framework of the ITSEC certification, then towards the end of this decade with the issue of global and public management of vulnerabilities and "malware" (security software vendors and CERTs). It is once again being developed at the present time with the recent release of log analysis and correlation tools that completely integrate this concept along with criticality.

severity level (of vulnerability or of nonconformity): The severity level definition is about the same as the one for incidents, with a few small differences:

- *Dangerousness*: impact of the related attacks, weakness of protective techniques, possible remote exploitation, scope of the target/victim population (number of machines, of services, etc.), importance to organization of the security rule that was violated.

- *Stealthiness*: same definition as for incident.

- *Exploitability* (by attackers), is the opposite definition of incident feasibility.

NOTE: The proposed definition is aligned with the CVSS (NIST SP 800-126 [2] or SCAP) standard for software vulnerabilities.

taxonomy: science of identifying and naming species, and arranging them into a classification

NOTE: The field of taxonomy, sometimes referred to as "biological taxonomy", revolves around the description and use of taxonomic units, known as taxa (singular taxon). A resulting taxonomy is a particular classification ("the taxonomy of ..."), arranged in a hierarchical structure or classification scheme.

threat: potential cause of an unwanted incident, which may result in harm to a system or organization

NOTE: There are 4 categories of threats:

- Natural threats:
    - Environmental causes: public service outage, fire, and other disasters
    - System failure: physical or software computer or network breakdowns

- Human threats:
    - Unintentional (error, carelessness, irresponsibility, unawareness, etc.): conception and design, development, operation and usage, due to chance, hasty development and deployment, tiredness, gullibility, incompetence
    - Internal or external malice: theft, economic spying, sabotage, intrusion, fraud, etc.

The frontier between error, carelessness and malice is often fuzzy: it is always possible for an unscrupulous employee to plead error even though he has been negligent or malicious. However the difference between unintentional and malicious actions can often be found with the following clues:

- An unintentional action is not hidden (so not stealthy), it tends to impact availability rather than confidentiality and integrity, and it has a low dangerousness and a high feasibility. The resulting severity is often low to fairly low.
- A malicious action is stealthier (notably to enable the attacker to remain anonymous and allow him to sustain the advantages obtained for a longer period of time), with an impact on confidentiality and integrity rather than on availability, and with high dangerousness.

trace: computer data that proves the existence of a business operation

NOTE: As an example, logs (see definition above) are traces, but traces are not necessarily logs.

vulnerability: undesirable state of a system whose occurrence or detection is a security event

NOTE: It corresponds to a flaw or weakness of an asset or group of assets (at the level of a technical system, process or behaviour) that can be exploited by a threat. Occurrence and actual detection of a vulnerability (often delayed in time) are considered the same in the present document. There are 6 types of vulnerabilities, but only the first four are in the scope of a SIEM approach and are being dealt with in the present document:

- Behavioural.
- Software (that can lead to malicious exploitation by an attacker via an "exploit").
- Security equipment or software configuration (same as above).
- General security technical or organizational (vulnerabilities defined as having a global and major effect on Information System's security level, and having a level equivalent to the 133 ISO/IEC 27002 [1] standard control points).
- Conception (overall system design at architecture and processes levels).
- Material level (corresponding with vulnerabilities which enable physical incidents - of an accidental, negligent or malicious kind).

A behavioural, configuration, global security (technical and organizational) or material vulnerability becomes a nonconformity (see definition above) when it violates the organization's security policy and rules. The present document uses the terms "usage or implementation drift" in this case.

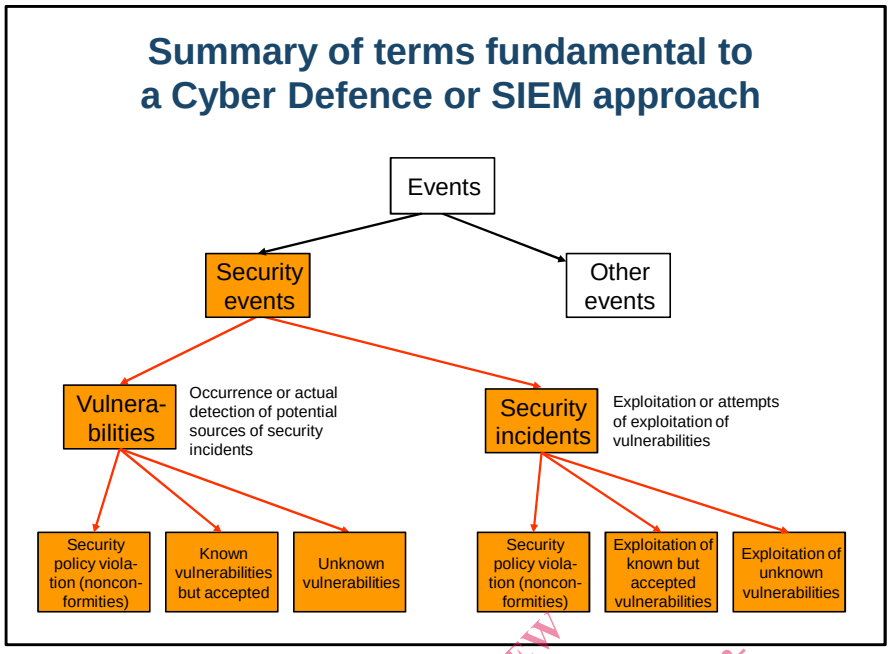

Figure 2: Relationships between different kinds of events

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

AD	Active Directory®
APT	Advanced Persistent Threat
CAG	Consensus Audit Guidelines
CAPEC	Common Attack Pattern Enumeration and Classification (Mitre)
CCE	Common Configuration Enumeration
CEE	Common Event Expression
CI	Computer Interface
CIA	Confidentiality Integrity Availability
CIO	Chief Information Officer
CISO	Chief Information Security Officer
COA	Courses Of Action
CSIRT	Computer Security Incident Response Team
CSS	Cross-Site Scripting
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
CWE	Common Weakness Enumeration
CybOX	Cyber Observable eXpression
DDoS	Distributed Denial of Service
DLP	Data Leak Prevention
DNS	Domain Name Server
DoS	Denial of Service
DPI	Deep Packet Inspection
HIDS	Host-based Intrusion Detection System
HTTP	HyperText Transfer Protocol
IDS	Intrusion Detection System
IP	Internet Protocol
IPS	Intrusion Prevention System
ISM3	Information Security Management Maturity Model
ISMS	Information Security Management System
ISO	International Organization for Standardization
IT	Information Technology
ITIL	Information Technology Infrastructure Library