ETSI GS ISI 008 V1.1.1 (2018-06)

Information Security Indicators (ISI); Description of an Overall Organization-wide Security Information and Event Management (SIEM) Approach

Disclaimer

The present 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-008

Keywords

cyber-defence, 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

The present document can be downloaded from:
http://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the only prevailing document is the print of the Portable Document Format (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
https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables 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 (https://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.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

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 9 ISI 00x specifications. These 9 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 [1] addressing (together with its associated guide ETSI GS ISI 001-2 [2]) information security indicators, meant to measure application and effectiveness of preventative measures.
- ETSI GS ISI 002 [3] addressing the underlying event classification model and the associated taxonomy.
- ETSI GS ISI 003 [i.1] addressing the key issue of assessing an organization's maturity level regarding overall event detection (technology/process/people) in order to weigh event detection results.
- ETSI 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).
- ETSI 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 ETSI GS ISI 003 one [i.1] and which can therefore complement it.
- ETSI GS ISI 006 [i.2] addressing another engineering part of the series, complementing ETSI GS ISI 004 and focusing on the design of a cybersecurity language to model threat intelligence information and enable detection tools interoperability.
- ETSI GS ISI 007 [i.3] addressing comprehensive guidelines to build and operate a secured SOC, especially regarding the architectural aspects, in a context where SOCs are often real control towers within organizations.
- **ETSI GS ISI 008 addressing and explaining how to make SIEM a whole approach which is truly integrated within an overall organization-wide and not only IT-oriented cyber defence.**

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

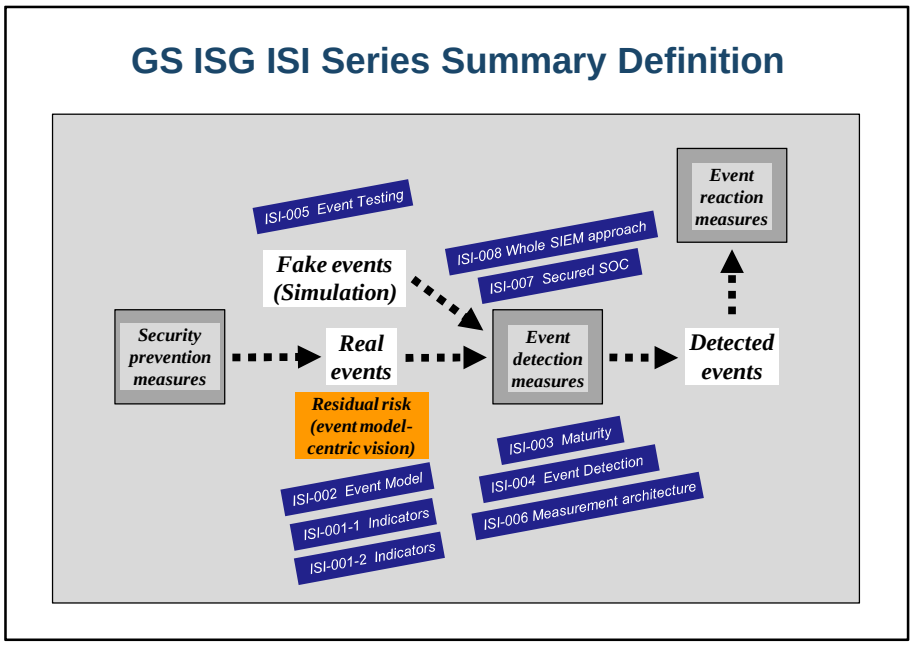

Figure 1: Positioning the 9 GS ISI against the 3 main security measures

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

The SIEM (Security Information and Event Management) field, which is an across the board outline to benefit from logs rolling up from various Information System security software packages (networks and servers), is now a well-known concept around the world. The very first SIEM projects in these countries in the years 2000, very often approached from a purely technical angle with no clearly defined at the outset security aims, highlighted the lack of feedback provided by these projects for companies. Thus, the first and true goal of a SIEM approach is to **check relevancy** of existing ISMS (Information Security Management System), and the SIEM project is the cornerstone of the ISMS architecture, in relation to its organizational, documentary, human, and technological aspects. The first concrete tendencies identified using this overall approach have shown that significant progress can be achieved within a few years (when there is an operational project on a company-wide basis).

With regard to ISMS relevancy checking, which should ensure the implementation of real security insurance throughout the organization, it is essential to make sure that the security policy is actually **enforced** and is **effective**. The **first aspect** involves monitoring of security practices compliance, in order to identify uses of the Information System not compliant to the established security rules, and to survey abuses of organization employees and partners more seriously. The **second aspect** means undertaken security investments effectiveness should be improved, in order to reduce the residual risks to which the company Information System is exposed, those remaining risks being not covered by existing preventative measures. Moreover, this close monitoring brings greater precision and significance to the awareness campaigns for employees and partners, because the messages of these campaigns can be adapted to deal with not compliant or deviant practises identified on the ground.

So there is a joint with cyber risks and general reference frameworks in kind of a **3-player game**, enabling to combine top-down and bottom-up approaches and to master the complexity and provide a real and tangible value to the overall scheme. In this context, the ETSI GS ISI 002 [3] event model and the associated ETSI GS ISI-001-1 [1] and ETSI GS ISI-001-2 [2] full set of indicators play a key and decisive role by being positioned at the crossroads of technical expertise and governance, and unleashing multiple uses either at the technical level or at the overall governance or management level.

1 Scope

The present document defines and describes the various concepts and areas of a whole SIEM approach, which involves SOCs, CSIRTs and Security governance teams.

A SIEM approach is usually associated with one or more of the following six major aims:

- To monitor in real-time security events, i.e. detection of those able to avoid existing preventative measures.
- To improve the communication and management of residual risks associated with previous security events, by means of the implementation of a reaction (immediate or not) and of protective measures.
- To ensure security policy enforcement, also called continuous checking (a term borrowed from the banking industry), by monitoring non-conformities and implementing feedback processes.
- To investigate security events with evidence collection, according to a code of practise called "forensic".
- To draw up detailed reports, using follow-up indicators which are often new and intended to complete existing security dashboards.
- To plan security, with the aim of streamlining the future security investments by measuring precisely the efficiency level of existing ones.

The target groups of the present document are heads of detection and reaction teams, heads of Cyber defence teams and heads of security governance (CISOs).

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 referenced document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at https://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.

[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] Security Indicators Quick Reference Card (V1.1.2).

NOTE: Available at https://sites.google.com/site/axelrennoch/specialities/security/isiQRC.pdf?attredirects=0.

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 referenced 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] ETSI GS ISI 003: "Information Security Indicators (ISI); Key Performance Security Indicators (KPSI) to evaluate the maturity of security event detection".

[i.2] ETSI GS ISI 006: "Information Security Indicators (ISI); An ISI-compliant Measurement and Event Management Architecture for Cyber Security and Safety".

[i.3] ETSI GS ISI 007: "Guidelines for building and operating a secured SOC".

[i.4] ISO/IEC 27002:2013: "Information technology - Security techniques - Code of practice for information security controls".

[i.5] ISO/IEC 27004:2016: "Information technology - Security techniques - Information security management - Monitoring, measurement, analysis and evaluation".

[i.6] ISO 27035-1:2016: "Information technology - Security techniques - Information security incident management - Part 1: Principles of incident management".

[i.7] ISO 27035-2:2016: "Information technology - Security techniques - Information security incident management - Part 2: Guidelines to plan and prepare for incident response".

3 Definitions, symbols and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in ETSI GS ISI 001-2 [2] apply.

3.2 Symbols

For the purposes of the present document, the symbols given in ETSI GS ISI 001-2 [2] apply.

3.3 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI GS ISI 001-2 [2] and the following apply:

CSIRT Computer Security Incident Response Team
KPSI Key Performance Security Indicators
SIEM Security Information and Event Management
SOC Security Operation Centre

4 The central position and pivotal role of an event classification model and associated indicators

The proposed classification model and its various uses are described in the ETSI GS ISI 002 [3]. This model is positioned at the heart of the "Risk management/ISO/IEC 27002 [i.4]/Cyber Defence and SIEM" scheme and is able to provide the central support (see clause 4 in ETSI GS ISI 001-2 [2]) of the implementation of such an overall scheme. Its strength results from the various ways in which it can be used, covering the full range of topics associated with a Cyber Defence and SIEM approach.

In the Quick Reference Card of Security Indicators [QRC v1.1.2:2015] [4] a classification scheme is summarized by descriptive identifiers according to the Common Criteria. This scheme describes Security Information in a hierarchical way using standardized identifiers for classes, component families, parameters values. Thus distributed SIEM processes can publish and subscribe various data types in a unique classified way.

5 Required reference frameworks and procedures in the framework of a SOC/CSIRT organization

The various uses explained in the ETSI GS ISI 002 [3] lead naturally to the need of a formalization of some of them, especially those not dealt with by existing reference frameworks or security methods. For concrete implementation, they need precise supports and guidelines which guarantee the coherence of the various domains of the SIEM/SOC/CSIRT approach. In addition to the event classification model itself, the following reference frameworks are necessary:

- Taking into account of SIEM aspects in security policies
- Glossary of terms usually used in the SIEM/SOC/CSIRT domains
- Follow-up indicators
- Reaction plans
- Associated legal aspects (forensic and privacy compliance)

The 1st reference framework, which is the base, the introduction and the unifying element of all other reference frameworks, aims to remedy usual loopholes in security policies for all SIEM-related areas. Based necessarily (in the light of their growing importance) on existing ISO/IEC 27002 [i.4], ISO 27035-1 [i.6] and ISO 27035-2 [i.7], it has to propose additions to operational aspects linked to detection and reaction to security events, and to deal with the following often neglected topics: production and recording of traces, automated evidence collection, operating modes, security dashboards and indicators, criticality level, reaction plans, escalation procedures, anomalies processing.

The 2nd reference framework is useful because a significant number of terms used in the SIEM domain are missing in ISO/IEC 27002 [i.4], ISO 27035-1 [i.6] and ISO 27035-2 [i.7], and therefore lack a common and recognized standard definition within the profession. This situation slows down awareness of SIEM approaches stakes and spreading of trustworthy concepts and practises. It is possible to translate the SIEM domain new main notions into a shared vocabulary coming from approaches common to the overall profession, a terminology which can be summarized in about twenty terms (see clause 3.1).

The 3rd reference framework deals with Information Systems security tables and dashboards, and its purpose is to provide and complete their content regarding indicators concerning mainly external and internal malice and internal deviant behaviors. It should cover precise threats which actually materialized (incidents) as well as systems, processes and users vulnerabilities and/or non-conformities. Its goal is to bring ISO/IEC 27002 [i.4] and its checking points (universal but sometimes a little theoretic and a little imprecise) closer to the real concrete situation on the ground. It should also complete and supplement ISO/IEC 27004 [i.5], more positioned on the methodology of indicators conception and measuring than on the precise selection of indicators themselves. This reference framework corresponds to ETSI GS ISI 001-1 [1].

The 4th reference framework aims to be a reference handbook for organizations' security teams in their approach in reacting to security events linked to error and malice, as well as partial material breakdowns (total material breakdowns giving rise to the launch of Business Continuity Plans, usually already in existence). It should consist of a full set of reaction plans which deal with all categorized events in the event classification model, those plans being written and formalized according to a shared model and by homogenous kinds. Its aim is to give a precise and immediately applicable content to ISO 27035-1 [i.6] and ISO 27035-2 [i.7] standards recommendations.

The 5th reference framework aims at setting out a complete overview of two domains (forensic, privacy compliance) closely linked to the legal area growing requirements, by focusing in particular on the relationship of those domains with SIEM approaches:

- To acquire a better knowledge of company employees and partners activities and behaviors, and to be able to provide undeniable evidence of possible deviant behaviors on their part.
- To protect employees and partners at the same time from drifts or potential abuses resulting from such an approach, using relevant organizational and technical arrangements, in accordance with and in application of local privacy laws.
- From these two complementary domains, to establish within the company a set of practises to rely on to help in achieving compliance with various new regulations and legislations (notably GDPR in Europe).

The first domain (called forensic) is a new discipline which deals with all operating modes and techniques used in legal investigations. In this domain, the reference framework role is to give precise execution directives to evidence collection and retention general action items, which are indicated in reaction plans.

6 Follow up indicators

6.1 User Security policy efficiency measurement with incidents follow up

A security policy efficiency mainly depends on the quality of controls implemented to protect the company from disasters with serious consequences and to limit frequency of less damaging or costly but more common disasters. The second aspect always involves the implementation of processes which control daily operations affecting the company information systems. These processes apply to the application software development field and to the production field. For the latter, the measures are technical, procedural and human, security incidents follow up allowing to appreciate first the relevancy of technical investments carried out in the prevention area and/or their concrete application. The role of organizational and human measures is also not insignificant, and their share of responsibility in incidents should therefore be constantly evaluated depending on types of incidents detected. Types of incidents concerned are first of all those with a significant impact on the goals in question and then the most frequent ones (according to statistical figures associated to the 98 indicators of ETSI GS ISI 001-1 [1]). ISO/IEC 27004 [i.5] gives on this issue interesting indications regarding indicators positioning in the PDCA model and ISMS context, notably on relevancy checking in relation to risk analysis and security policy, and more precisely on residual risk measurement. These considerations are of a crucial importance in a SIEM approach regarding the choice of monitoring areas and priorities, and this awareness determines to a considerable extent the feedback which may be expected from the approach.