ETSI GS ISI 007 V1.1.1 (2018-12)

Information Security Indicators (ISI); Guidelines for building and operating a secured Security Operations Center (SOC)

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-007

Keywords

cyber defence, 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 efficacy 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 [i.2] 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.3] addressing ways to produce security events and to test the efficacy 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.4] addressing another engineering part of the series, complementing ETSI GS ISI 004 [i.2] and focusing on the design of a cybersecurity language to model threat intelligence information and enable detection tools interoperability.
- **ETSI GS ISI 007 (the present document) 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 [i.5] 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.

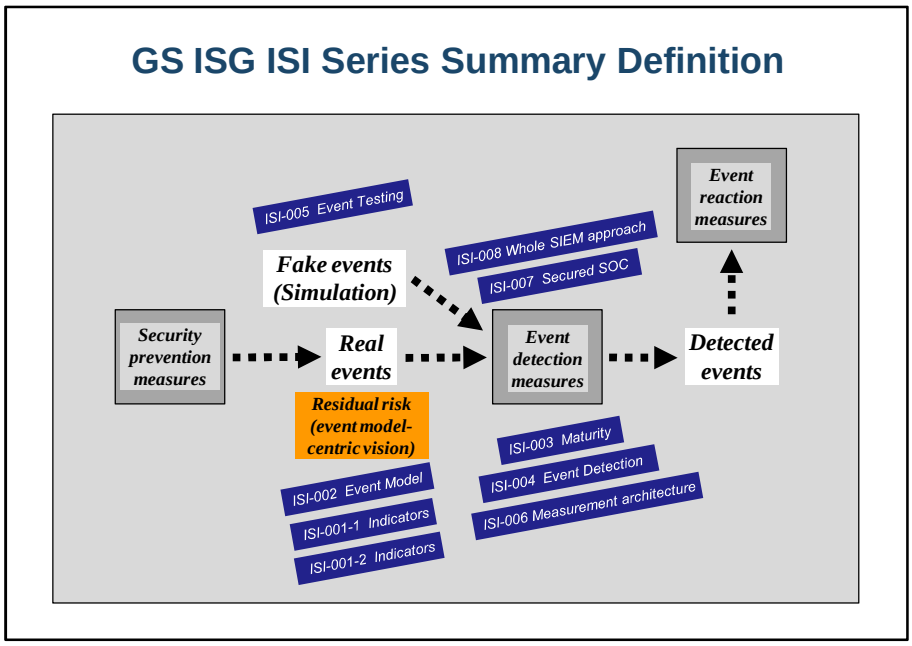

Figure 1: Positioning the 9 GS ISI against the 3 main security measures

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 growing interconnection of networks and the requirements of dematerialization leave information systems vulnerable to cyber-attacks. The points of interconnection with external networks and, in particular, with the Internet, are all access points an external attacker can attempt to exploit to enter and remain inside an information system in order to steal, alter or destroy its information assets. And addressing often very dangerous internal threats is also necessary.

Furthermore, new regulations and laws make it more and more mandatory to detect and report to authorities security incidents. This is in particular the case with the **Network and Information Security (NIS) Directive [**i.10**]**, for which the present document can be a strong basis for the implementation of Articles 14 and 16. For this purpose, it addresses a secured way to use cyber threat intelligence to detect security incidents, which is an important issue to be dealt with in the NIS Directive.

The use of security incident detection systems contributes to the protection of information systems from the threats of cyber-attacks. Human, technical and organizational resources can be concentrated within a cyber security operations center (CyberSOC or SOC), generally dedicated to the detection of and response to security incidents. Depending on the challenges, needs and resources of the commissioning entity, this center can be internal, outsourced dedicated or even shared. In this latter case, the pooling of resources can have positive effects, such as the sharing of information on threats and detection rules.

When the provision of the detection service is compliant with the state-of-the-art, and is precisely adapted to the needs of the commissioning entity, it helps to prevent severe security incidents (by detecting vulnerabilities or non-conformities - see ETSI GS ISI 001-1 [1] or ETSI GS ISI 002 [3]) or, when such incidents occur, to limit their consequences by making it possible to take rapid remediation actions that can be carried out by the commissioning entity's security incident response teams (located either in a CERT or in the SOC itself).

However, the concentration and pooling of detection capabilities make the cyber security operations center a prime target for attackers. Therefore, special attention should be paid to protecting its information system.

The purpose of the present document is to provide guidelines to build and operate a **secured SOC**, through a list of functional, organizational and technical requirements. Furthermore, it covers **security incident detection** up to incident reporting to the commissioning entity **without entering the incident response field**.

It can also be used, in the interest of adopting best practices, independently of any regulatory framework.

1 Scope

The present document covers the 2 types of security incident detection services: internal and external.

The requirements can be implemented at 2 different levels: basic level (partial compliance), advanced level (full compliance).

The present document is structured as follows (after clauses 2 and 3 respectively dedicated to references and terms, symbols and abbreviations):

- **Clause 4** describes the activities to which the present document relates.
- **Clause 5** presents the requirements applicable to service providers (either internal or external) operating a SOC.

NOTE: These requirements, labelled with lowercase letters (a, b, c, etc.), stem from requirements of a similar reference framework published by ANSSI [i.12], so that their labelling is aligned with them, meaning that not present letters correspond to discarded or not relevant requirements.

- **Annex A** presents the tasks and skills expected from the service provider's employees.
- **Annex B** presents the recommendations for the commissioning entities when contracting with security incident detection providers.
- **Annex C** defines the basic and partial level of implementation of the requirements.

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

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 004: "Information Security Indicators (ISI); Guidelines for event detection implementation".

[i.3] ETSI GS ISI 005: "Information Security Indicators (ISI); Guidelines for security event detection testing and assessment of detection effectiveness".

[i.4] ETSI GS ISI 006: "Information Security Indicators (ISI); An ISI-compliant Measurement and Event Management Architecture for Cyber Security and Safety

[i.5] ETSI GS ISI 008: "Information Security Indicators (ISI); Description of an Overall Organization-wide Security Information and Event Management (SIEM) Approach".

[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".

[i.8] ANSSI: "Guide d'hygiène informatique".

NOTE: Available at https://www.ssi.gouv.fr/entreprise/guide/guide-dhygiene-informatique/ for an up-to-date version.

[i.9] The Center for Internet Cybersecurity: "Critical Security Controls for Effective Cyber Defense Version 7".

NOTE: Available at https://www.cisecurity.org/critical-controls.cfm.

[i.10] Directive (EU) 2016/1148 of The European Parliament and of The Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

NOTE: Available at https://eur-lex.europa.eu/eli/dir/2016/1148/oj.

[i.11] ISO 27000: "Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary".

[i.12] ANSSI (The French Networks and Information Security Agency): "Security incident detection service providers - Requirements reference document".

NOTE: Available at https://www.ssi.gouv.fr/uploads/2014/12/pdis_referentiel_v1.0_en.pdf.

3 Definition of terms, symbols and abbreviations

3.1 Terms

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

NOTE: They are primarily taken from the ISO 27000 [i.11] and ISO 27035 [i.6] and [i.7] standards.

administrator: member of the detection service with privileged rights enabling them to ensure the smooth running of the detection service devices

collection source: equipment within the information system that generates events related to the security of the information

collector: device enabling the centralization of security events originating from various collection sources

EXAMPLE: Syslog server, SIEM solution collector.

NOTE: In the context of this service, local collectors are collectors installed in the commissioning entity's information system, and central collectors are collectors used for centralizing events and located in the service provider's information system.

commissioning entity: entity using a security incident detection service

context of a security incident: event related to a security incident, along with all information analysed and produced during its qualification

EXAMPLE: Qualification analysis report(s).

detection rule: list of technical elements allowing identifying an incident based on one or more events

NOTE: A detection rule can be formed by one or more markers, one or more signatures or a behavioural rule based on abnormal behaviour. A detection rule can originate from the vendor of the technical analysis tools used for the detection service, the service provider itself (monitoring of new incidents, a rule used for another commissioning entity with its agreement, etc.), a partner, a specialized supplier, or it can have been created specifically for the commissioning entity.

efficacy: level of achievement of planned activities and the expected results

information system: organized set of resources (hardware, software, personnel, data and procedures) for processing and communicating information

investigation: process designed to collect and analyse all technical, functional or organizational elements of the information system in order to qualify a suspicious situation as a security incident and to understand the intrusion set and the scope of a security incident within an information system

operator: member of the detection service in charge of operating the service, i.e. performing the detection-related tasks constituting the service on behalf of the commissioning entity

probe or detection system: technical device designed to identify abnormal, suspicious or malicious activity within the supervised perimeter

NOTE: The purpose of a probe is to generate security events; it is considered to be a collection source within the security incident detection service.

qualified service: security incident detection service provided to a commissioning entity in compliance with the reference document

qualifying a security incident: determining the nature and criticality of a security incident

reporting: act of informing the commissioning entity of the occurrence of a security incident jeopardizing its information system

security of an information system: all technical and non-technical controls that make it possible for an information system to manage events that could compromise the availability, integrity or confidentiality of the data being handled or transmitted and the related services that this system provides or makes available

service agreement: written agreement between a commissioning entity and a service provider for the performance of the service

NOTE: When the service provider is a private entity, the service agreement includes the contract form.

service provider: entity providing a security incident detection service in compliance with the present document

state-of-the-art: set of publicly accessible best practices, technologies and reference documents (and the information that can be inferred from them) relating to information systems security

NOTE: These documents can be made available on the Internet by the information systems security community, or distributed by reference or regulatory entities.

subcontracting: operation through which the service provider entrusts to another entity all or part of the execution of a contract concluded with the commissioning entity

supervised perimeter: all or part of the commissioning entity's information system, which is object of the security incident detection service

third party: person or organization that is recognized as independent from the service provider and the commissioning entity

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:

ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information (France)
CERT	Computer Emergency Response Team
CIS	Center for Internet Security
IS	Information System
ISI	Information Security Indicators
NIS	Network and Information Security
SLA	Service Level Agreement
SOC	Security Operations Center

4 General Description of the Security Incident Detection Service provided by the SOC

4.1 Activities of the security incident detection service

The security incident detection service is composed of three distinct activities:

- Incident management, meaning all of the technical and organizational means for identifying and qualifying a security incident on the basis of collected events. Storing and capitalizing on security incidents in order to improve the service is also part of this activity.
- Event management, meaning all technical and organizational means for ensuring the collection and storage of security events.
- Reporting management, meaning all technical and organizational means making it possible to inform the commissioning entity about detected security incidents and to store these reports.

Reaction and remediation activities are beyond the scope of this service.

4.2 Architecture of the detection service information system

The present document does not impose any specific architecture on the detection service's information system. Several implementation methods are possible. In particular, according to the type of detection service (internal or external), the different zones presented in this clause can be hosted in different entities or organisms, provided that the requirements of the present document are complied with.

Figure 2 is a simplified representation of a typical architecture for a security incident detection service information system, provided for informational purposes only.

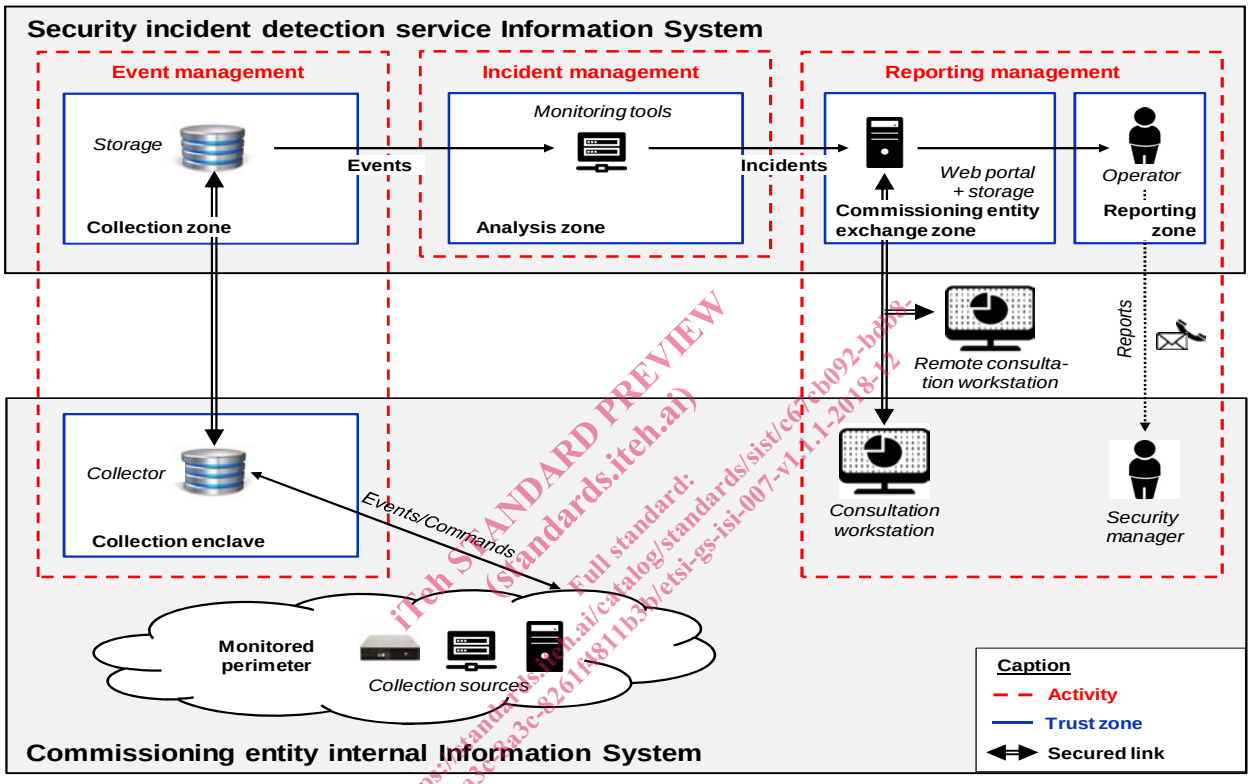

Figure 2: Simplified representation of a typical architecture for a security incident detection service information system

The information system of a detection service is organized into trust zones, partitioned using filtering, authentication and access control mechanisms. The trust zones in the information system of the detection service are the following:

- collection zone(s) (one or more), comprising all devices involved in the collection process, including the central collectors and the systems for storing events and, where necessary, background information;
- analysis zone(s), comprising all devices involved in the analysis process, including the technical tools for analysing security incidents;
- reporting zone(s), comprising commissioning entity's reporting systems, in particular messaging systems;
- commissioning entity exchange zone(s), comprising all devices enabling the commissioning entity to view the details of information on the reported incidents, in particular the web portal, and to provide, where applicable, the information necessary to qualify the incident;
- administration zone(s), comprising all administration tools and administration workstations;
- update zone(s), comprising all devices involved in the process of downloading updates for detection service devices;