ETSI GS ISI 003 V1.2.1 (2018-01)

Information Security Indicators (ISI); Key Performance Security Indicators (KPSI) to evaluate the maturity of security event detection

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
RGS/ISI-003rev_2

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

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 4
Foreword 4
Modal verbs terminology 5
Introduction 5
1 Scope 6
2 References 6
2.1 Normative references 6
2.2 Informative references 7
3 Definitions, symbols and abbreviations 7
3.1 Definitions 7
3.2 Symbols 7
3.3 Abbreviations 7
4 Background 8
4.1 Key Performance Indicators 8
4.2 Key Performance Security Indicators 8
4.3 SANS CAG 9
5 Key Performance Security Indicators 10
5.1 How to use KPSIs to assess the organization's overall maturity level in security event detection and response posture 10
5.2 How to use KPSIs as a first step to evaluate the detection levels of security events 10
5.3 KPSIs description table 11
5.4 Description of the relevant KPSIs 11
Annex A (normative): Recap of available KPSIs 16
Annex B (informative): SOC example 18
Annex C (informative): Authors & contributors 26
History 27

Intellectual Property Rights

Essential patents

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 (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 specifications. These 9 specifications are the following (see figure 1 summarizing the various concepts involved in event detection and interactions between all specifications):

- 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: addressing the key issue of assessing an organization's maturity level regarding overall event detection (technology/process/ people) and to evaluate event detection results.**
- ETSI GS ISI 004 [4]: 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.1]: addressing ways to produce security events and to test the effectiveness of existing detection means within an organization. More detailed and more a case by case approach than the present document and therefore complementary.
- ETSI GS ISI 006 [i.2]: addressing another engineering part of the series, complementing 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 [i.4]: 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.

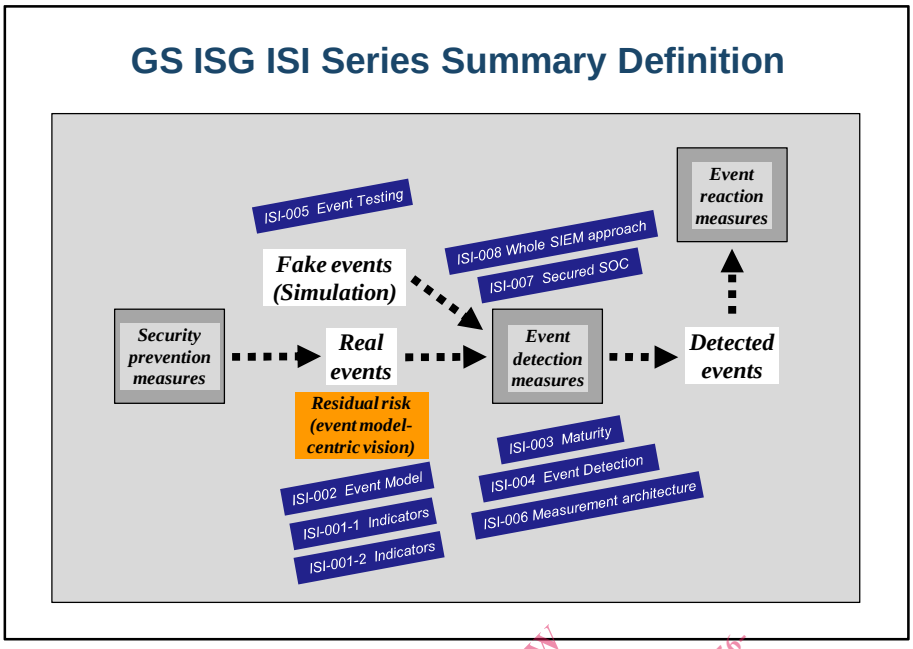

Figure 1: Positioning the 9 GS ISI against the 3 main security measures

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 present document addresses the event detection aspects of the information security processes in an organization. The maturity level assessed during event detection can be considered as a good approximation of the overall Cyber Defence and SIEM maturity level of an organization.

1 Scope

The present document defines and describes a set of Key Performance Security Indicators (KPSI) to be used for the evaluation of the performance, the maturity levels of the detection tools and processes used within organizations for security assurance. The response is not included in the scope of the present document.

In particular, the purpose of the present document is to enable organizations to:

- assess the overall maturity level of the security event detection;
- provide a reckoning formula to assess detection levels of major security events as summarized in ETSI GS ISI 001-1 [1];
- evaluate the results of measurements.

This work is mainly based on the CIS® Controls [5].

The target groups of the present document are Head of detection, reaction teams, Cyber defence team and head of security governance.

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

[5] CIS® Controls V6.1.

NOTE: Available at https://www.cisecurity.org/controls/ for an up-to-date version.

[6] 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 005: "Information Security Indicators (ISI); Guidelines for security event detection testing and assessment of detection effectiveness".

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

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

[i.4] ETSI GS ISI 008: "Information Security Indicators (ISI); Description of a whole organization-wide SIEM approach".

[i.5] The Capability Maturity Model Integration CMMI® V1.3 (Software Engineering Institute/Carnegie Mellon University, 2001).

NOTE: Available at https://resources.sei.cmu.edu/asset_files/presentation/2011_017_001_23331.pdf.

[i.6] OGC PSM3® V2.1: "Portfolio, Programme and Project Management Maturity Model (2008).

NOTE: Available at http://miroslawdabrowski.com/downloads/P3M3/OGC%20branded/P3M3_v2.1_Introduction_and_Guide.pdf.

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:

CC	Critical Control
CMMI	Capability Maturity Model Integration
CSIRT	Computer Security Incident Response Team
KPI	Key Performance Indicators
KPSI	Key Performance Security Indicators
MSSP	Managed security service provider
SOC	Security Operation Centre

4 Background

4.1 Key Performance Indicators

Key Performance Indicators (KPIs) are quantifiable variables which can measure the performance of an organization, evaluate the success of specific activities and support decision making processes. KPIs are metrics that allow to measure progress and deficiency. The metrics have to be well-defined and quantifiable to be useful.

KPIs can be used to assess the performance of IT services. Examples of IT KPIs are the availability of IT systems and services, the Service Level Agreements (SLAs), the Mean Time Between Failures (MTBF) and the Mean Time To Recover (MTTR), and Mean-Time-Between-System-Incidents (MTBSI).

The usage of KPI in the field of Information Assurance is at its early stage. Defining KPIs for the Security Assurance processes is difficult because of the complexity of regulations, certifications, technical and organizational issues, and budget constraints. Hence it is a complex task to quantify clear Security Assurance objectives and performance in terms of KPIs.

4.2 Key Performance Security Indicators

Key Performance Security Indicators (KPSIs) can measure the maturity level of the information security processes (detection and detection-related processes).

A Maturity Model to measure the performance in the Security Assurance field can be based on the five level maturity framework adapted from The Capability Maturity Model Integration CMMI® (Software Engineering Institute, 2001) [i.5] and Portfolio, Programme and Project Management Maturity Model P3M3® (OGC, 2008) [i.6]. Organizations using these models, can assess the maturity level of their performance management practices in the five dimensions of the model:

1) **Initial:** Processes are managed ad hoc. No measure of the performance is requested.

2) **Managed:** Processes characterized for projects and are often reactive.

3) **Defined:** Processes are tailored for the organization and are proactive.

4) **Quantitatively Managed:** Processes are measured and controlled.

5) **Optimizing:** Continuous Process Improvement.

To adapt these models to security event detection and detection-related reactions, a simplified 3-level scale is proposed:

- The present document, level 1 corresponding to CMMI® levels 1 and 2.
- The present document, level 2 corresponding to CMMI® levels 3 and 4.
- The present document, level 3 corresponding to CMMI® level 5.

The three levels can be defined as follows:

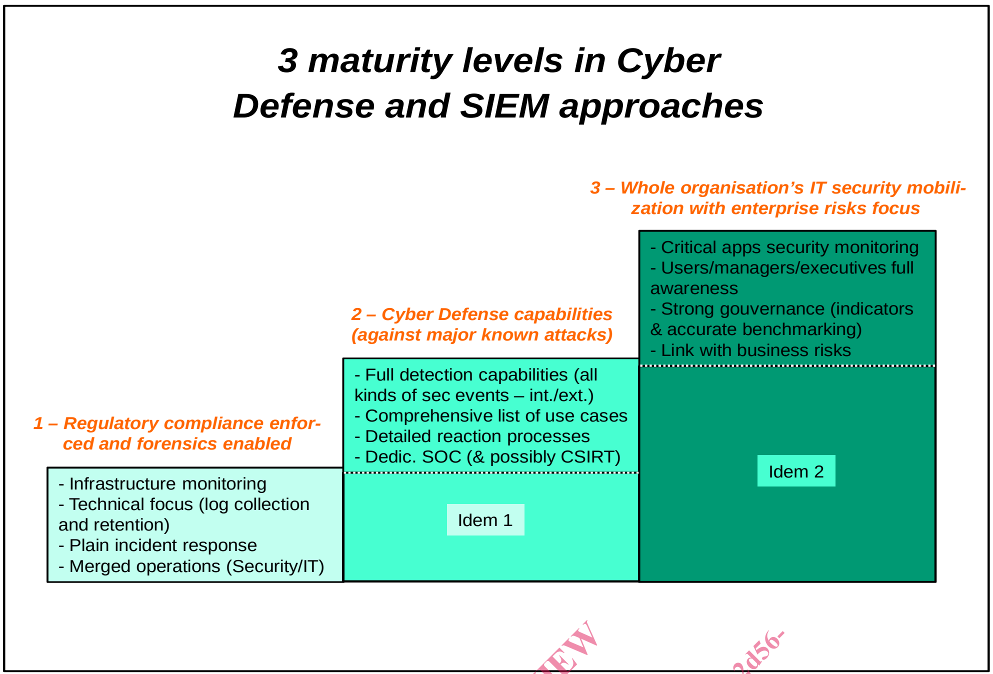

Figure 2: 3 majority levels in Cyber Defence and SIEM approaches

4.3 SANS CAG

The CIS Controls [5] is a compliance standard that specifies 20 "control points" that have been identified through a consensus of security professionals from the federal and private industry. The aim is to begin the process of establishing a prioritized baseline of information security measures and controls that can be applied across organizations to help improving their defences.

The 20 Critical Controls subject to collection, measurement, and validation currently defined are:

1) Inventory of Authorized and Unauthorized Devices.
2) Inventory of Authorized and Unauthorized Software.
3) Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers.
4) Continuous Vulnerability Assessment and Remediation.
5) Malware Defences.
6) Application Software Security.
7) Wireless Device Control.
8) Data Recovery Capability (validated manually).
9) Security Skills Assessment and Appropriate Training to Fill Gaps (validated manually).
10) Secure Configurations for Network Devices such as Firewalls, Routers and Switches.
11) Limitation and Control of Network Ports, Protocols and Services.
12) Controlled Use of Administrative Privileges.
13) Boundary Defence.
14) Maintenance, Monitoring, and Analysis of Security Audit Logs.

15) Controlled Access Based on the Need to Know.

16) Account Monitoring and Control.

17) Data Loss Prevention.

18) Incident Response Capability (validated manually).

19) Secure Network Engineering (validated manually).

20) Penetration Tests and Red Team Exercises (validated manually).

Each Critical Control (CC) is described in detail, is subject to continuous monitoring and checking and has gained a broad consensus as regards their relevancy and effectiveness.

The KPSIs defined within the present document are based on the CC list concerning detection, with adaptation and extension whenever needed to cover the scope of the ETSI ISG ISI series.

5 Key Performance Security Indicators

5.1 How to use KPSIs to assess the organization's overall maturity level in security event detection and response posture

The first purpose of KPSIs is to assess the organization's overall maturity level of security event detection and response posture. The way to do it is to reckon the average of all KPSIs in order to get the unique level for the whole organization, which can then be compared to the best in the industry.

5.2 How to use KPSIs as a first step to evaluate the detection levels of security events

The second purpose of KPSIs is to enable an organization to assess the actual detection levels of security events as summarized in ETSI GS ISI 001-1 [1] information security indicators and to evaluate the results of the measurements.

The formula to reckon the actual detection level of events is by making an indicator from the following: state-of-the-art detection level (see ETSI GS ISI 001-1 [1]) x organization KPSI/state-of-the-art KPSI.

To apply this formula, it is of course required to know which KPSI(s) is (are) applicable to the given indicator. This requirement is met below in clause 5.4 for each indicator (see the row "Core ISI 001 mapping" [1] for a minimal indicators mapping, and "Additional ISI 001 mapping" [1] for a full mapping of the indicators over the KPSIs). When an indicator has several KPSIs assigned, it is proposed to take the average of all of them to get a unique and finalized KPSI.

All data necessary to use the formula are given for each KPSI in clause 5.4 with a recap in annex A.