ETSI GS ISI 005 V1.1.1 (2015-11)

GROUP SPECIFICATION

Information Security Indicators (ISI); Guidelines for security event detection testing and assessment of detection effectiveness

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-005

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
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:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

Copyright Notification

Contents

List of figures

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 specifications.
These 6 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 [i.8] addressing (together with its associated guide ETSI GS ISI 001-2 [i.12]) information security indicators, meant to measure application and effectiveness of preventative measures,
- ETSI GS ISI 002 [i.9] addressing the underlying event classification model and the associated taxonomy,
- ETSI GS ISI 003 [i.11] addressing the key issue of assessing an organization's maturity level regarding overall event detection (technology/process/ people) in order to evaluate event detection results,
- ETSI GS ISI 004 [i.10] 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 test the effectiveness of existing detection means within an organization, which is a more detailed and a more case by case approach than ISI 003 [i.11] one and which can therefore be complementary.

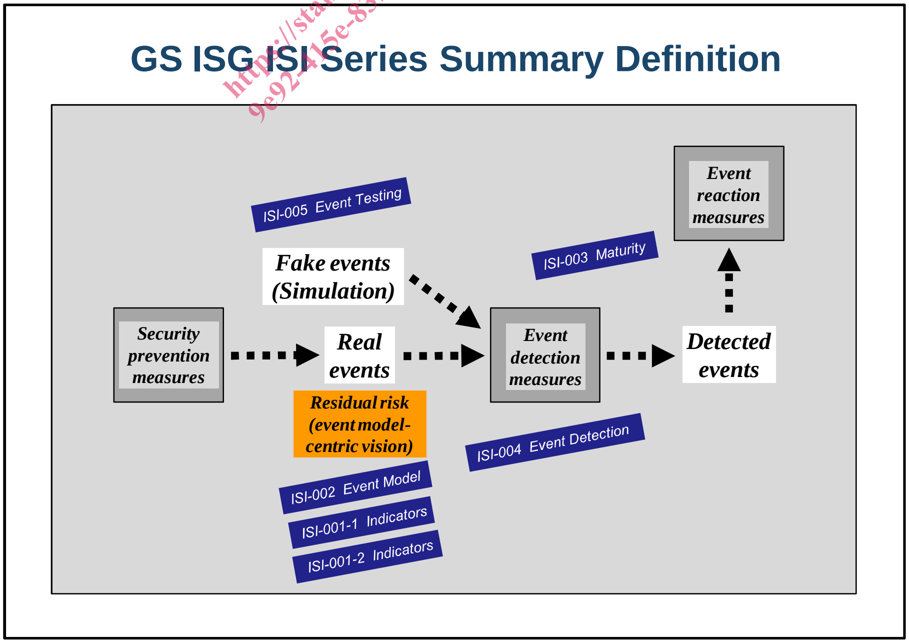

Figure 1: Positioning the 6 GS ISI against the 3 main security measures

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 purpose of the present document is to describe strategies and techniques to test security event detection systems and to assess the effectiveness of such systems.

The present document also includes few examples of tests scenarios.

1 Scope

The present document provides an introduction and guidelines for the development of tests to check the capabilities of security event detection systems.

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 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.

The following referenced documents are necessary for the application of the present document.

Not applicable.

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] ISO 27004:2009: "Information technology - Security techniques - Information security management - Measurement".

[i.2] ISO/IEC/IEEE 29119-2: "Software and system engineering - Software Testing - Part 2 : Test process, 2013".

[i.3] IEEE 829™-2008: "Standard for Software and System Test Documentation".

[i.4] Recommendation ITU-T X.294: "OSI conformance testing methodology and framework for protocol Recommendations for ITU-T applications - Requirements on test laboratories and clients for the conformance assessment process".

[i.5] ISO/IEC 15408: "Information technology -- Security techniques -- Evaluation criteria for IT security".

[i.6] Common Weakness Enumeration (CWE).

NOTE: Available at https://cwe.mitre.org.

[i.7] Common Attack Pattern Enumeration and Classification (CAPEC).

NOTE: Available at https://capec.mitre.org.

[i.8] 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.9] ETSI GS ISI 002: "Information Security Indicators (ISI); Event Model A security event classification model and taxonomy".

[i.10] ETSI GS ISI 004: "Information Security Indicators (ISI); Guidelines for event detection implementation".

[i.11] ETSI GS ISI 003: "Information Security Indicators (ISI); Key Performance Security Indicators (KPSI) to evaluate the maturity of security event detection".

[i.12] 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.13] DIAMONDS project deliverables.

NOTE: http://www.itea2-diamonds.org/_docs/D3_WP4_T1_v1_0_FINAL_initial_test_patterns_catalogue.pdf.

[i.14] A. Vouffo Feudjio:"A Methodology For Pattern-Oriented Model-Driven Testing of Reactive Software Systems", PhD Thesis, February 2011.

NOTE: http://opus.kobv.de/tuberlin/volltexte/2011/3103/pdf/vouffofeudjio_alaingeorges.pdf.

[i.15] OWASP-AT-003: "Testing for Default or Guessable User Account".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in ETSI GS ISI 001-1 [i.8] and the following apply.

stimulation: single or sequence of activities in order to produce a security event: security incident (e.g. installation of an unauthorized application) or introduction of a vulnerability (e.g. misconfiguration of a critical device)

system under test: security event detection system or software to be tested

system under monitoring: system where the security event detection system is installed

test case: set of conditions or variables under which a tester will determine whether a system under test satisfies requirements or works correctly

test pattern: expression of the essence of a well-understood solution to a recurring testing problem

test priority: level of (business) importance assigned to a test case

test selection: means of adapting Test Suites to the options supported by the Implementation and/or the priorities provided by the test developers, customer or other stakeholders or algorithms [i.4]

3.2 Abbreviations

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

AV	AntiVirus
CAPEC	Common Attack Pattern Enumeration and Classification (Mitre)
CCHIT	Certification Commission for Health Information Technology
CIA	Confidentiality Integrity Availability
CPU	Central Processing Unit
CVE	Common Vulnerabilities and Exposures
CWE	Common Weakness Enumeration
DNS	Directory Name Service
DOS	Denial of service
EICAR	European Expert Group for IT-Security
HTTP	Hyper Text Transfer Protocol
IDS	Intrusion Detection System
IETF	Internet Engineering Task Force
IPS	Intrusion Prevention System
ISO	International Organization for Standardization

IT	Information Technology
NIST	National Institute of Standards and Technology (USA)
OS	Operating System
PC	Personal Computer
PIN	Persona Identification number
SFR	Security Functional Requirement
SIEM	Security Information and Event Management
SQL	Structured Query Language
SSL	Secure Socket Layer
SUT	System Under Test
TCP	Transport Control Protocol
UML	Unified Modelling Language
URL	Uniform Resource Locator
XML	Extensible Markup Language

4 Objectives of security event detection testing

4.1 Assessment of detection effectiveness

4.1.0 Introduction on assessment of detection effectiveness

The objective of testing security event detection systems is to be able to assess the effectiveness of the detection functionality. This evaluation can be performed in a laboratory (the detection system under test is not connected to an operational system) or in real operation (the detection system under test is connected to the real operational system).

Detection capability testing can be done before the deployment of the detection system. Test campaigns can also be organized regularly to assess the sustainability of the detection capability.

It should be noted that when detection capabilities are outsourced, specific audit clauses have to be defined in the contract.

The result of the assessment is not a single result but a set of both quantities and qualitative data.

4.1.1 Examples of quantitative results

4.1.1.1 Detection level

This measurement determines the rate of security events detected correctly by the SUT in a given environment during a particular time frame. The accuracy of that detection level is directly based on the sample of events used to perform the measurement. Due to the fact that as of today no standardized sample database exists, current published detection levels are not comparable between each other.

The other reason why results are not comparable is due to the fact that the detection level is directly linked to the detection rules configured in the tools (IDS, SIEM). The list of configured rules depends on each particular deployment and not on the installed tools.

4.1.1.2 Coverage of events specified in ETSI GS ISI 001-1

ETSI GS ISI 001-1 [i.8] specifies a list of events that may be detected in order to generate accurate indicators. The measurement of the detection level could be the amount (in percent) of security events that the system under test can detect compared to the list specified in the ETSI GS ISI 001-1 [i.8].

4.1.1.3 False-positive rate

This measurement determines the rate of false-positives produced by a detection system in a given environment during a particular time frame. A false-positive or false alarm is an alert caused by an event that is not a security event (vulnerability or incident).

4.1.2 Examples of qualitative results

Testing can also be used to characterize the type of detection implemented in the system under test. Detection type can be categorized in three main categories:

- Suspicious behaviours (exhibited either by targets or attackers) that deviate from usual and specified operations (also known in the literature as "anomaly detection").
- Exploitation underway of known software or configuration vulnerabilities (also known in the literature as "misuse detection").
- Other attacks requiring correlation (especially known structured and complex attack patterns).

Clause 6 of ETSI GS ISI 004 [i.10] provides more details on the technical characteristics of these three categories.

4.2 Conformity evaluation

For benchmarking or for procurement purpose, it could be necessary to evaluate the conformity of a security event detection system to its specifications. Specifications can include the list of security events that the system is able to detect or the list of sensors (collecting data) supported by the system.

If the detection system is limited to a product, the Common Criteria standard methodology [i.5] can be used to evaluate the conformity of the product to its specifications (its "security target" in the Common Criteria terminology).

4.3 Resistance to attacks

Another objective of the testing of a security event detection system could be to evaluate its resistance to attacks. To be efficient, the detection system should, either be unreachable by the attackers, or at least more resistant and resilient than the system under monitoring. It is therefore accurate to evaluate the resistance of the detection system to attacks.

The main objective of attacking a detection system is to deactivate detection capabilities. That objective can be reached:

1) by physical attacks on the equipment supporting the detection;

2) by software attacks on servers or probes.

If the detection system is limited to a product, the Common Criteria standard methodology [i.5] can also be used to evaluate the resistance of the product to attacks. The standard defines four levels of resistance:

1) the product is resistant to attacks performed by an attacker possessing Basic attack potential (AVA_VAN.1 & AVA_VAN.2 assurance requirements components [i.5]);

2) the product is resistant to attacks performed by an attacker possessing Enhanced-Basic attack potential (AVA_VAN.3 assurance requirements components [i.5]);

3) the product is resistant to attacks performed by an attacker possessing Moderate attack potential (AVA_VAN.4 assurance requirements components [i.5]);

4) the product is resistant to attacks performed by an attacker possessing High attack potential (AVA_VAN.5 assurance requirements components [i.5]).

5 Test framework

5.0 Introduction

This clause addresses general consideration for testing, i.e. test procedures, configurations that are needed to perform test campaign of detection systems. When applicable they have been derived and/or adopted from appropriate security testing activities [i.5].

5.1 Active vs. passive testing

Technically, the detection system should trigger over the presence of a certain type of security event. That event can be artificial (the tester generates the event, there in-after "Active testing") or the tester can wait for the occurrence of a real event (for example: the tester waits for the publication of a vulnerability in one of the deployed system, there-in-after "Passive testing").

The biggest benefit of the active testing is that it is not necessary to wait for the occurrence of real security events. Moreover, it could be impossible to test the detection of events having a very low probability of occurrence. The other difficulty is that the test should be aware of the occurrence of the security event even if it was not triggered by the SUT. It means that the tester needs another detection system with a better detection than the SUT in order to identify when the SUT does not detect what it should.

5.2 Active testing by stimulation

5.2.1 Objectives

As explained before, testing of security event detection capabilities is more accurate using active testing, when feasible. The objective for the tester is here to stimulate the detection procedures and mechanisms through the injection of events in the system under the monitoring of the detection system.

The tools and techniques used by the tester to stimulate the detection system are described in clause 6 of the present document.

5.2.2 Testing strategy

To make the interpretation of results easier, tests scenarios should be elaborated to trigger as much as possible a single security event detection. But to be representative of operational conditions, normal system activity should also be present.

While testing in the operational environment generates naturally such conditions, special activity generators should be developed for testing in labs.

Depending on the objective of the test campaign (detection effectiveness measurement, conformity evaluation, resistance to attacks), different testing strategies should be elaborated.

5.2.3 Stimulation location

5.2.3.0 Introduction on stimulation location

A tester can stimulate the SUT in two different ways: by the creation of the event or by the creation of the effects of the event. In addition, the tester should create « noise » simulating normal system usage in order to verify if the detection system is able to extract accurate events symptoms in that noise.