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

GROUP SPECIFICATION

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

Copyright Notification

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.

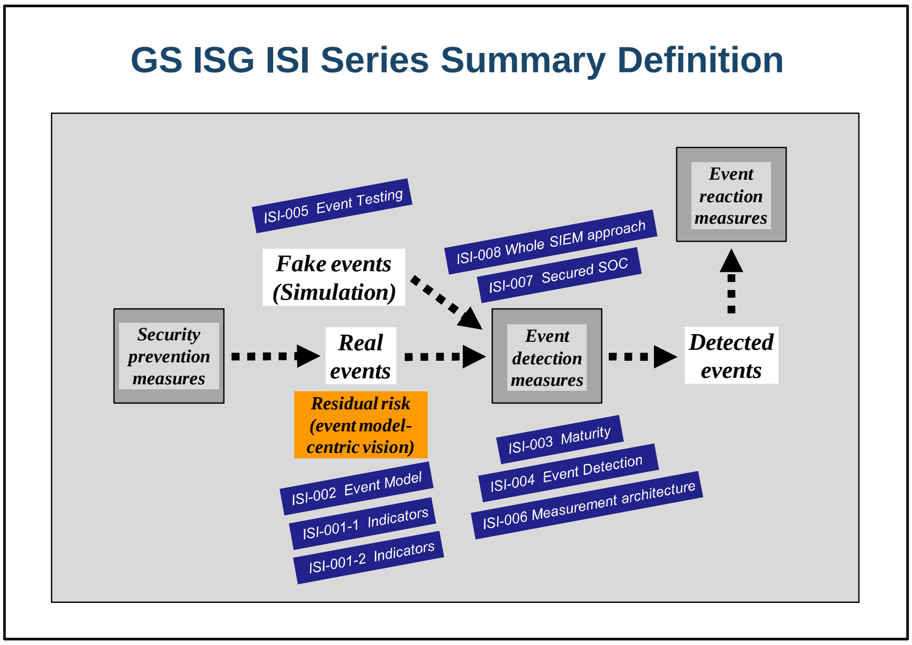


Figure 1: Positioning the 9 GS ISI against the 3 main security measures

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.

6.2 User security practices follow up

One of the main feedbacks noticed in organization-wide SIEM approaches is user behaviors new knowledge (employees, partners and external service providers). Security events follow up at this level fits in "Internal deviant behaviors" (IDB) and "Behavioral vulnerabilities" (VBH) classes of the ETSI GS ISI 002 [3] event classification model. Security events concerned here are either incidents or vulnerabilities or non-conformities (if they explicitly contravene security rules in force). The pursued goal is to spot abuses or deviant behaviors from Information System authorized users, in order to provide a relevant response. Human weaknesses in question and at the source of these events are of three types: simple and sheer error, carelessness and malice (greed or revenge). These internal human weaknesses, whether they cause disasters directly or indirectly (through weakening or removal of the security of some Information Systems, which are later exploited), are responsible for over 70 % of all detected security incidents. On this point, a specific group of people should be subject to particular attention; this one consists of network, system or security administrators, directly or indirectly responsible for 15 to 18 % of security incidents. This close follow-up makes possible to envision a pre-established relevant reaction in the case of serious incident and to guide precisely and appropriately user awareness campaigns, with support of real facts and events. The first way could be the opportunity to let those concerned know about the security policy key elements and about security rules concerning the dealt with situation, and to ask them to propose possible suggestions for their improvement and to contribute always to information transmission in their immediate circle. The second way is notably applicable to all minor incidents, and it makes full use of statistical bases designed in order to analyse from a behavioral and contextual point of view user practices and drifts (depending on functions, geographical zones, determined periods, etc.). This last aspect and central issue will result on a longer term in the establishment of an objective base to be used by Counter Competitive Intelligence initiatives within organizations.

6.3 Vulnerabilities and/or non-conformities follow up in a continuous checking

Within an organization, to be sure of the implemented ISMS relevancy, the security policy and rules actual enforcement should first be examined. This enforcement should be checked either on a sporadic basis by setting up targeted audits (Periodic Checking), or on a continuous basis (Continuous Checking). Continuous Checking concerns everything related to **constant monitoring** of human, technical or procedural vulnerabilities. **Continuous checking** may be organized according to 3 main categories:

- That concerning software and configuration (technical) vulnerabilities and/or non-conformities (ETSI GS ISI 001-1 [1] and ETSI GS ISI 001-2 [2] VSW and VCF classes).
- That concerning behavioral (human) vulnerabilities and/or non-conformities, which represents a sub-set of the area described in the previous clause 6.2 (ETSI GS ISI 001-1 [1] and ETSI GS ISI 001-2 [2] VBH class).
- That concerning general and related to ISMS (technical and organizational) vulnerabilities and/or non-conformities (ETSI GS ISI 001-1 [1] and ETSI GS ISI 001-2 [2] VOR class).

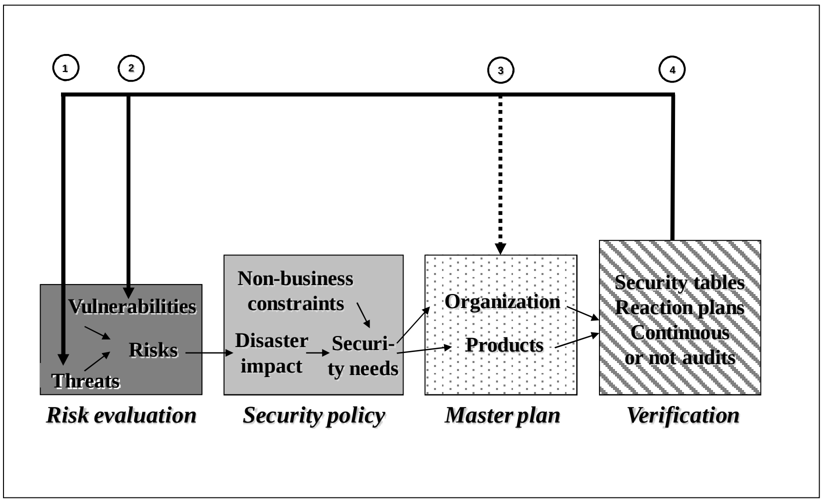
It should be pointed out here that (configuration, behavioral and general) vulnerabilities become non-conformities when they violate the security policy. Share of Continuous Checking compared to the one of Periodic Checking can be estimated from the ISO/IEC 27002 [i.4] control points; one third of the total is generally concerned in the best current projects at international level. Moreover, Continuous Checking generally offers a sufficient coverage with roughly sixty precise events (typical breakdown being 25 % for software vulnerabilities, 30 % for configuration vulnerabilities, 25 % for behavioral vulnerabilities, and 20 % for general vulnerabilities). For about half of these, an automated follow-up under the monitoring of a SIEM tool is possible.

With respect to the crucial issue (mentioned in the previous clause 6.1) of choosing ideal monitoring areas and priorities for a SIEM tool, Continuous Checking generally provides almost 70 % of all detected security incidents, a further example of the interest to take into consideration this specific use of SIEM tools.

7 Reaction to security events

7.1 Necessity of a reaction

The reaction to security event issue, which aims to improve existing insufficiencies and lacks as regards checking, is taking on new dimensions today in organizations. Figure 2 indicates the different types of reaction which can be implemented using verification and detection means available to security managers (security dashboards, periodic or continuous audits, incident monitoring and exposure to attacks).



1) Incident processing (in real or delayed time).
2) Vulnerabilities and/or non-conformities processing (in real or delayed time).
3) Improvement of security processes and rules, optimization of existing preventative tools parameters, user awareness.
4) Compilation of Information Security Indicators.

Figure 2: Different types of reaction

The 4th type of reaction (at SOC or Governance levels) may consist in identifying unusual trends for some measurements or comparing indicator results with previous results and with state-of-the-art statistical figures to decide which kind of reaction is required.

The 3rd type of reaction illustrates ISMS improvement (the Act of the PDCA model, notably developed in ISO/IEC 27002 [i.4]), made possible thanks to experience feedback learned through security incident constant follow-up (ISMS efficiency measurement). This improvement can be organized in a structured way, using several complementary actions of various rationales:

- Based on periodic audits results during security steering committees.
- During security steering committees, based on trends identified in security dashboards, by relying on indicators which are, in the case of SIEM approaches, more complete and often more precise than previously.
- As part of reaction plan step 5, partly dedicated to lessons to be learned (see below and clause 7.4).

The 1st and 2nd types of reaction can be achieved in the framework of strictly formalized reaction plans, launched in real or delayed time in the case of significant or critical security events. The necessity and interest of such reaction schemes can be summarized as follows:

- It enables addressing and taking in charge residual risk, which is not covered by or dealt with successfully by preventative measures, although it may be critical in many cases.
- It makes it possible to deal with underway attacks, before a disaster actually becomes evident.

- It allows, every time a plan is launched following an internal security event, security awareness of employees and/or organizations' business partners and external service providers (with the aim of improving user behaviors and promoting security policy key elements).
- It corresponds to ISO/IEC 27002 [i.4] recommendations.

The decision to launch or not a plan should however be guided widely by business considerations, as many situations which are not critical or merely internal can be dealt with by security equipment or software periodic updates and simple awareness campaigns based on SIEM tool provided irrefutable statistics.

7.2 Interest of a reference framework of reaction plans

Once security events have been detected, identified and precisely categorized, it may be essential to set off as soon as possible a relevant sequence of actions, in order to remedy existing or potential consequences from these events. Given the large number of existing events (standard or specific to an organization), question arises to **limit** as far as possible the **number** of different reaction plans, by trying to gather the maximum of homogenous events as regards relevant processing to be applied (at the organizational processes level). The interest for a backing by a reference framework for that purpose seems therefore obvious and turns on the following points:

- Capitalization on best practices encountered on the international level (Experience has shown that more than 90 % of events can be dealt with using a standard reaction plan from a reference framework, and that only 7 % of unknown or not categorized events, called anomalies, require a specific processing as explained in clause 7.5. Furthermore, 90 % of launched plans are carried out completely on the first attempt and are therefore fully successful).
- Alignment with the ETSI GS ISI 001-1 [1] security event classification model (and therefore related statistics).
- Decisive contribution to allow security managers to take up their duties as regards security event processing.
- Harmonization of response in order to be able to measure it.
- Cost-cutting in reaction plans implementation.

The experience gathered in most advanced SIEM projects have shown that the whole reaction scheme could be fully covered by some thirty different plans.

7.3 The criticality level of security events

The core of a SIEM approach consists of security event processing. Forming into a hierarchy and prioritizing events are vital requirements from both security and economic points of view, thus introducing the criticality definition. Interest and the main uses of criticality are the following:

- When qualifying a security incident, it enables to launch a course of actions using reaction plans with a strength in line with the threat intensity (relevant stress applied to organization).
- It also allows to come up with an optimal cost/efficiency ratio for this reaction.
- It accounts for distinction between an underway attack and a disaster which has really occurred.
- It makes it possible to work out objective statistics on the true threats and disasters, thus providing a dependable representation and understanding of the threat hanging over the organization.

The **criticality level** of a security event is determined by its severity (inherent to the event itself - see below) and by the sensitiveness of the target attacked or concerned (linked to the asset estimated value for the company - which value concerns the confidentiality, the integrity or the availability).

The **severity level of a security incident** is generally defined on a 4-level scale inherent to the event itself and that depends on several criteria that vary according to the types of events. These criteria are the following (in decreasing order of importance):

- *Dangerousness* is resulting from several objects with variable combinations according to circumstances or types of incidents: execution or spreading speed, virulence, effectiveness, scope and number of impacted assets, capability of harm and of target reach, capability of remotely acting, persistence, weakness or lack of curative means, and last depth which is can be or has been reached (concept of Defence in Depth or DiD).

- *Stealthiness* has several levels: obvious visibility, discretion but can be seen by basic means, detection by advanced technical tools, almost invisibility. It is a key factor within the framework of monitoring and detection concerns. Anonymization and camouflage active and passive means are stealthiness means. Stealthiness takes on an indirect meaning insofar it applies to similar not yet detected incidents.

- *Feasibility* is in relation to the attacker's motivation and in inverse ratio to the sum of the necessary means (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 evolution: actually, if a hacking tool is difficult to be created, once it is available on Internet, it can be used by not seasoned criminals. Feasibility takes on an indirect meaning insofar it first applies to potential threat (see definition of this term), but it gives good clues on several amongst its components, including criminals' actual capability.

A measurement standard for the criticality level should be defined (with the scale used and the meaning of its different levels), by relying on the sensitiveness scale described in the security policy.

The most advanced SIEM products integrate totally this criticality concept, by taking into account all or part of the previously mentioned criteria in order to compute in real time the criticality level of each detected event.

7.4 Reaction plans description

The reaction plans should be described and formalized according to a shared model and by unified types, in order to ease their readability and their absorption to the various players involved. The proposed model is a five step model, which is applied to all the plans (with the exception of the plans concerning the software and configuration vulnerabilities, which contain five stages with a different content). These steps are the following (see figure 3):

- Security incident identification and confirmation (alerting managers concerned, establishing the criticality level of security incident, deciding whether or not to launch plan).

- Attack isolation or containment to limit its consequences and damages, in order to spare possible spread.

- Detailed analysis of harm and of possible violations of security rules in force, traces and evidence collection.

- Examination of the best way to return to normal, restoration of usual operations, and stopping of the alarm.

- Assessment of whether or not sensitive information has been disclosed, lessons to be learned (update of the affected security or system software, possible improvement of security rules, need for awareness strengthening, etc.), coercive measures to be taken (legal action, negotiated approach regarding a partner, disciplinary action, etc.).

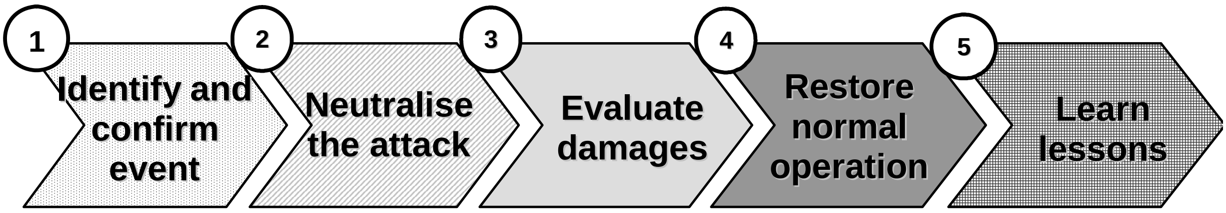


Figure 3

The reaction plans concerning the software and configuration vulnerabilities (which are generally and for most cases launched **once a week or a month**, unlike other plans launched in real time) are organized according to the following five stages:

- Vulnerability detection, qualification and analysis (discovered either after an external warning, or after an internal vulnerability scan, or after a security event having exploited and revealed it).
- Identification of servers or PCs affected by the vulnerability (non priority reaction process which is postponed if the sensitiveness level of impacted assets is low, process to be carried out within 24 hours in the opposite case).
- Selection of applications and systems to be modified and information of the managers concerned.
- Intervention planning (patch management or configuration change), patch (or configuration) test and installation as soon as available.
- Intervention checking.

Each plan should propose several different reaction levels depending on the criticality level of the corresponding event (with actions of varying levels of extent and disturbance). The number of practical relevant levels is 3. In this case, plans are launched only for highly critical events (level two or three), level one (lowest level) in principle and with very few exceptions leading to an awareness program. Feedbacks from company-wide SIEM projects show that launching plans is only necessary for 1 to 2 % of all detected events. Moreover, a large number of critical events concern incidents involving plain users without specialized skills; therefore, they require accessed systems hardening rather than organization of a systematic reaction, preventative measures very often turning out to be the most efficient way of dealing with risks faced.

7.5 Processing of non standard situations

It is essential to define an appropriate response when a reaction plan under progress turns out to be not sufficient to solve the problem and return to normal. In this case, an action carried out in accordance with the plan together with its detailed technical refinements does not generate the expected effect. The operation agent may then be faced with a situation for which planned normal and standard measures (tools and processes) alone are not enough; he has to resort to more powerful measures and a higher level of decision. Also known as an escalation procedure, an emergency plan then needs to be launched.

This process is also applicable to a second case. Security events can be classified in two categories: known events and unknown events. The first category concerns identified and ETSI GS ISI 002 [3] categorized events (incidents or non-conformities), for which perfectly defined reaction plans exist. The second one concerns security events with which there are no established reaction plans, events which are known as anomalies. In this case, the operating agent should also envision launching an escalation procedure.

The criteria to decide further actions to the launch are the following:

- An event which the operating team is unable to categorize.
- No significant result following the application of a standard reaction plan during a planned period of time.
- High sensitiveness level of affected system.
- Event affecting a very large Information System area.

When a security operation agent is facing a situation to which one of the 2 first criteria applies, as well as one of the 2 last criteria listed above, he should immediately let an Information Security manager know to decide on how best to proceed with the operations. If a serious problem has been confirmed, the escalation procedure is pursued by an ad-hoc meeting of the crisis team, in order to decide on appropriate actions. Feedbacks from organization-wide SIEM projects show that these non-standard situations happen for about 7 % of security events, and that escalation procedures goes to term in one out of ten cases.

8 SIEM approach contribution for meeting regulations and legislations

The amount of regulations and legislations in the world today has outburst, regardless of whether it is specific or not to a particular industry. This fact has direct consequences on companies or governmental and public services Information System security. In most cases, the role of a SIEM approach can be summarized by the following three aspects:

- Constant checking of security policy application, which means a continuous decision-taking whether the policy is applied or not.
- Continuous tracking and taking into account of residual risk.
- Provision of relevant evidence.

The experience accumulated on the matter has shown that the minimal field of monitoring in order to ensure respect of concerned regulations and legislations is the following:

- Network security equipment and infrastructure of perimeter (firewalls, IDS/IPS, routers, VPN, reverse proxies, directories, DNS and DHCP).
- Perimeter dynamic Web and e-business servers.
- Servers and software applications concerned by the regulation.
- Possible internal and/or external exchanges between concerned software applications.

Main legislations or regulations concerned are the following: laws related to the protection of the critical infrastructure, laws related to privacy protection (follow-up of applications which deal with personal data), laws dedicated to digital economy trustworthiness (companies and public services protection as regards internal and external malice), laws requiring employees connection data retention (organizations protection against external complaint as regards their employees' behavior).

The contribution of SIEM approaches is mainly based on increased insurance that it attains for the security level claimed by the organization. And on this point, the specific contribution of a complete and strictly implemented architecture of reference frameworks is to reinforce these guarantees and these insurances. The positioning of reference frameworks in this whole context is described by the 4-level figure 4, which illustrates their assigned role to fill the gap between the general security frameworks and the technical tools (SIEM and others).

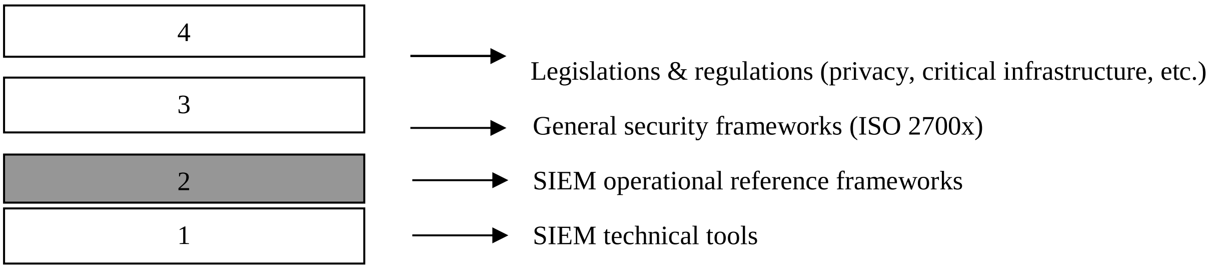

4
3
2
1
Legislations & regulations (privacy, critical infrastructure, etc.)
General security frameworks (ISO 2700x)
SIEM operational reference frameworks
SIEM technical tools

Figure 4: Positioning of reference frameworks

9 Legal aspects of a SIEM approach

9.1 Evidence collection

Although it is still too soon to speak with certitude on case laws which are only just emerging, a solid supposition can be made concerning a valid proof definition, with certain features common to most current legislations and regulations. In general, rules defining a proof validity cover (see ISO/IEC 27002 [i.4]):

- How it is perceived (is it accepted as an element worthy of consideration by the legal world).

- The value it represents (its application quality and extent).

With regard to the second aspect, issues requiring examination concern the necessary precautions to support and reinforce the validity of the evidence provided. This concerns the warranty of integrity of the recorded traces, whether recording processes are documented and audited, later access to recordings in the presence of a bailiff, necessity of operating on mirror copies and not on the original for all research and investigative purposes. The field of application of these general recommendations (which is « forensic » one) concerns all recorded information and evidence on a magnetic or software data-storage device, and is limited to immaterial field.

There is a countless amount of possible uses with these investigation techniques, but the most frequent scenarios are the following:

- External intrusion with economic or strategic espionage motivation.
- Non-authorized disclosure (intentional or accidental) of confidential information by an employee or an external service provider, which violates a regulation or a legislation, giving rise to legal complaint by third party and resulting in proving limitation of the company's own liability.
- Internal or external fraud, aiming at goods or money misappropriation.

9.2 Privacy protection

Company Information System users systematic monitoring also involves the need to protect these users against potential abuses and drifts associated with such a process, by means of relevant organizational arrangements and techniques. GDPR (EU General Data Protection Regulation) defines principles to be respected as regards collection, treatment and storage of company employees and frequent partners personal data. GDPR compliance in a SIEM approach is a way of demonstrating transparency and trust towards employees, as well as a guarantee of security from a legal point of view for human resources or legal managers and, more generally, for concerned organization's heads and managers. Following issues have to be addressed:

- Owner of the application in question.
- Aim and objective of the processing.
- Security rules and tools implemented for data protection.
- Description of recorded data, of the management process of their life cycle (up to their destruction) and of their retention duration.
- Measures taken to let those concerned know about their rights and possibly get their consent.
- Measures allowing those concerned to exercise their access rights.

Data in question (recorded in the SIEM tool central database) are at least data concerning daily connections or electronic messaging exchanges. Moreover, the possible recording of the subject and/or the content of exchanged messages is generally protected by other laws.

Regarding internal steps about user information, a basic recommendation is to rely on councils representing workers to provide explanations on the organization security monitoring practices (for external partners and service providers, contracts governing the relationship between the organization and these groups should contain writings on this matter). It is also necessary to ensure the confidentiality of identity data and access control and cryptography related data, and to grant access to these data only to the following positions: SOC (Security Operations Centre) members and Human Resources managers (Purchasing or Sales for external partners and service providers). Furthermore, those in these positions should be made relevantly aware, for issues under their own responsibilities, of the organization's executives' liability with regard to the law (professional secrecy).

10 Towards a necessary balance as regards prevention and reaction

Regarding relevant controls necessary to reduce a risk considered unacceptable by the organization, there are three types of possibly applicable measures:

- Preventative measures, the aim being to prevent the actual occurrence of an already identified risk or the appearance of a disaster (or otherwise at least to reduce the probability of it happening).
- Detection measures, the aim being the early detection of security incidents in order to be able to react and deal with them efficiently.
- Protective measures, the aim being to cancel or limit the disruption and various consequences on organization operations (for example, Business Continuity Plans in the case of breakdown).

These three types of measures are complementary and are sometimes implemented all together to cope with a given risk. Detection and protective measures should also be considered as a means of tackling residual risk, which is not taken into account by preventative measures. Although only residual, this risk can in some cases be a serious threat to the organization financial health. Detection measures therefore deserve the same general attention as preventative measures. Furthermore, the balance between the three types of measures should also take into consideration the necessity of minimal disturbance of organization business or activities. Finally, implementation of all these measures should be proportional to the expected disaster-related cost reduction. It is therefore necessary to consider a number of criteria in order to decide on a suitable balance between prevention, detection and protection. The current trend, especially due to the growing opening of organizations' Information Systems, is towards the reinforcement of access and exchange monitoring in order to lessen the impact of the increased vulnerability of traditional preventative means in this new context (mainly access control with passwords).

11 Conclusions

A number of current SIEM projects, considered with too much emphasis on the technical dimension, have demonstrated only poor provision to organizations, and failures with these complex technology projects are still frequent. Several surveys by consulting firms on typical difficulties encountered in SIEM products implementation (having found fully convergent results) have highlighted the existence of a link between SIEM approaches difficulties or failures and slightness of security aspects dedicated to these operations. The main two errors noted are the lack of specifications dedicated to security (70 % of cases) as well as the lack of a steering committee representative of the main functions involved in SIEM project (58 % of cases). Security specifications is the document which allows defining precisely checking aspects, by relying totally on detailed risks hanging over the organization and on existing security policies. And use of some reference frameworks described in the current specification is a significant aid in this crucial exercise.

Significant overall progress in security can be attained by implementing an organization-wide SIEM approach, as shown by other surveys. The results, presented according to the ISO/IEC 27002 [i.4] main directions, highlight notable advances for some of those directions, especially with regard to incident management, compliance, human resources security and asset management.

The incident detection and response products market is one of the fastest growing segments of the security market. This current tendency is directly linked to hope within organizations that these new investments will help them to better master ever more diversified risks to which their Information Systems are exposed.

This hope is legitimate in light of feedbacks from the most advanced present SIEM/SOC/CERT projects, especially those one concerning actual improvement of user behaviors regarding security. Moreover, the road to success in an organization-wide SIEM approach is today perfectly mapped out with regard to monitoring perimeters and objectives and to be implemented throughout organization processes. All conditions are therefore gathered to pave a new way in the Information Systems security field and get away from sheer qualitative (and not quantitative) approaches, which often hinder the security domain actual efficiency. And measurement comprehensiveness and accuracy will finally allow to better direct efforts and to maximize returns on investments.

Annex A (informative): Authors & contributors

The following people have contributed to the present document:

Rapporteur:
Gerard Gaudin, G²C, Chairman of ISG ISI

Other contributors:
Herve Debar, Institut Telecom, Vice-Chairman of ISG ISI

Arnaud Fillette, Thales, Secretary of ISG ISI

And in alphabetical order:

Jan deMeer, SmartSpaceLabs.eu

Axel Rennoch, Fraunhofer Fokus

Philippe Saadé, ESI-Group

Julien Saugeot, BNP Paribas

History

Document history		
V1.1.1	June 2018	Publication