# ETSI GS ISI 004 V1.1.1 (2013-12)


# Information Security Indicators (ISI); Guidelines for event detection implementation

***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-004

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

# Contents

# 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 multi-part specifications. These 6 specifications are the following (see figure 1 summarizing the various concepts involved in event detection and interactions between all specifications):

- GS ISI 001-1 addressing (together with its companion guide GS ISI 001-2) information security indicators, meant to measure application and effectiveness of preventative measures,
- GS ISI 002 addressing the underlying event classification model and the associated taxonomy,
- GS ISI 003 addressing the key issue of assessing organisation's maturity level regarding overall event detection (technology/process/people) and to weigh event detection results,
- 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),
- 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 ISI 003 one and which can therefore complement it.

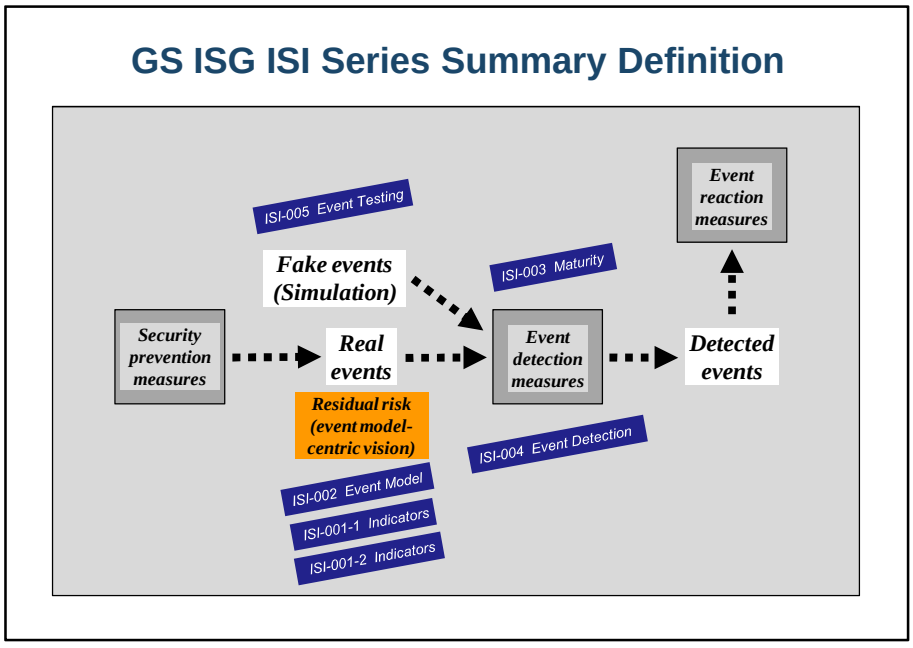


**Figure 1: Positioning the 6 GS ISI multi-parts against the 3 main security measures**

# Introduction

The purpose of the present document, which is the engineering part of the ISG ISI 5-part series, is to:

- present a comprehensive classification of the main symptoms/use cases (in some cases also referred to as indicators of compromise) to look for in IT system traces in order to detect stealthy events (as listed in GS ISI 002 [i.3]);
- position all these elements of information within a consistent framework (MITRE CybOX standard) in order to ease their exchange between various security stakeholders (such as CSIRTs, SOCs, administrators, etc.);
- give some examples of frequent security events in order to illustrate powerful means and methods of detection.

The present document addresses only events detected through technical means, and only security incidents and behavioural vulnerabilities, excluding all other kinds of vulnerabilities (software, configuration and general security), since these latter are far simpler to detect with well-identified and well-established methods and tools. And regarding security incidents, focus is stressed mainly on attacks of a malicious nature.

# 1 Scope

The scope of the present document is to define and describe a classification of the main symptoms/use cases, which are used to detect security events listed in GS ISI 002 [i.3].

# 2 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.

## 2.1 Normative references

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

[2] NIST SP 800-126 Revision 2 (September 2011): "The Technical Specification for the Security Content Automation Protocol (SCAP Version 1.2)".

## 2.2 Informative references

[i.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".

[i.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".

[i.3] ETSI GS ISI 002: "Information Security Indicators (ISI); Event Model: A security event classification model and taxonomy".

# 3 Definitions and abbreviations

## 3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

NOTE: See also the summary chart at the end of this list.

**asset:** entity (information or physical component) that has value to the organization and that can be broken down in primary assets (such as business activities, data, application software, etc. which hold the business value) and secondary/supporting assets (network or system infrastructure, which host primary assets)

**assurance:** planned and systematic activities implemented in a management system so that management requirements for a service will be fulfilled

NOTE: It is the systematic measurement, comparison with a standard, monitoring of processes and an associated feedback loop that confers error prevention. This can be contrasted with Management "Control", which is focused on process outputs.

**base measure:** regarding the "indicator" definition, defined in terms of an attribute and the specified measurement mean for quantifying it (e.g. number of trained personnel, number of sites, cumulative cost to date)

NOTE: As data is collected, a value is assigned to a base measure.

**continuous auditing:** periodic verification and collection of a series of controls identified within the Information System, corresponding to the detection of incidents and of software, configuration, behavioural or global security framework vulnerabilities and/or non-conformities

NOTE: There are three auditing levels (in principle, hierarchy notably implemented within banking and financial institutions):

- Detailed behavioural, global security framework or technical checking at the security software or equipment level (network, system, application software).
- Level 1 auditing via monitoring of trends and deviations of a series of significant measurement points.
- Level 2 auditing (verification of existence of an appropriate level of assurance and technical coverage of the chosen control and measurement points, and of implementation of regulatory requirements).

Continuous auditing can be either manual or automatic (for example, monitoring by means of tools appropriate for a SIEM approach). Finally, continuous auditing is generally associated with statistical indicators (levels of application and effectiveness of security controls), that provide information regarding the coverage and assurance level of the security controls in question.

**criticality level (of a security event):** level defined according to the criteria which measures its potential impact (financial or legal) on the company assets and information, and which make it possible to evaluate the appropriate level of reaction to the event (incident treatment or vulnerability or nonconformity removal)

NOTE: The criticality level of a given event is determined by the combination of its severity level (inherent to the event itself - see definition below) and of the sensitiveness of the target attacked or concerned (linked to the asset estimated value for the company - whose value concerns confidentiality, integrity or availability). This concept of criticality level (usually defined on a scale of four levels) is at the core of any SIEM approach, for which classifying security events processing according to organization-defined priorities is vital from both a security and economic point of view.

**derived measure:** regarding the "indicator" definition, measure that is derived as a function of two or more base measures

**effectiveness (of security policy or of ISMS):** As a supplement to the actual application of security policy (or of ISMS) and of its measures assessment, it is necessary to assess its level of effectiveness, that can be estimated through identified residual risk (that corresponds with the residual vulnerabilities that are actually exploited and that have led to security incidents).

NOTE: It should be added that the term "efficiency" is sometimes also used, but generally with a different meaning of economy in the use of resources (not addressed here for reasons of lesser relevancy).

**(security) incident:** single unwanted or unexpected security event, or series thereof, that correspond to the exploitation of an existing vulnerability (or attempt to), and with an actual or potential threat (attempt underway), that have a significant probability of compromising business operations and threatening information security

NOTE: In case of success, an incident affects nominal operations of all or part of an information system (according to the Confidentiality, Integrity and Availability criteria - English acronym CIA). An incident that manifests itself through previously unseen phenomena, or is built as a complex combination of elementary incidents often cannot be qualified and therefore inventoried or categorized easily; such an incident will often be referred to as an anomaly.

**indicator:** measure that provides an estimate or evaluation of specified attributes derived from an analytical model with respect to a defined information need

NOTE: Indicators are the basis for analysis and decision making.

**log:** continuous recording of computer usage data, with specific characteristics: detailed and specified structure, time-stamping, recording as soon as they occurs in files or other media

NOTE: Logs are a kind of trace (more general concept - see definition below).

**non-conformity:** security event that indicates that organization's required security rules and regulations have not been properly enforced, and are therefore the consequence of a usage or implementation drift

NOTE: Continuous monitoring of non-conformities (similar to continuous auditing - Cf. this term above) enables to better ensure that an organization's security policy is being enforced. Non-conformity can be further refined according to their kind: configuration, behaviour, global security (technical and organizational) and material. Non-conformities are also vulnerabilities or incidents, depending on the situation (see definition).

**periodic audit (Periodic scanning):** using isolated audit means, periodic acquisition and verification of security controls

NOTE: A periodic audit can also be either manual or automatic (for example, carried out through scanner type tools). Finally, a periodic audit is generally Boolean (all or nothing compliance level).

**risk:** product of the probability of occurrence of a security incident involving a specific asset by its impact on this asset (impact assessed according to the CIA sensitivity level)

NOTE: The level of risk exposure (concept which is used in risk assessment methods) corresponds to the product of the vulnerability level of the asset in question by the threat level hanging over it.

**risk not covered (by existing security measures):** Risk sometimes also referred to as "residual", which breaks down into 3 shares:

- Known and realized suffered risk, corresponding to the impact suffered by the organization under attack when the security policy is not applied (configuration, behavioural or global security non-conformities), and when known and critical software vulnerabilities are not appropriately addressed.
- Known and accepted risk that corresponds to a risk taken by choice by an organization, by comparing the risk associated with attacks with economic, usage and security level considerations.
- Unknown risk associated with unknown and unpatched vulnerabilities, or innovative attack vectors.

**security event:** information about a change of state in a system that may be security relevant and that indicates the appearance of a risk for the organization

NOTE: A security event is either an incident or a vulnerability occurrence or detection (see definition of these terms). 500 security events have been inventoried within the industry, and are grouped into 7 major categories, with the 3 first corresponding to incidents, and the 4 last to vulnerabilities: external attacks and intrusions, malfunctions, internal deviant behaviours, behavioural vulnerabilities, software vulnerabilities, configuration vulnerabilities, general security (technical or organizational) vulnerabilities.

**Security Information and Event Management (SIEM) solutions:** combination of the formerly separated product categories of SIM (security information management) and SEM (security event management)

NOTE 1: SEM deals with real-time monitoring, correlation of events, notifications and console views. SIM provides long-term storage, analysis and reporting of log data.

NOTE 2: The present document extends these two notions under the generic SIEM acronym, which encompasses all organizational, processes and human aspects necessary to deploy and operate these tools, and which include vulnerability and nonconformity management; we may refer to Cyber Defence approaches in the most complex case.

**security policy:** overall intention and requirements as formally expressed by management

NOTE: Two levels are used: general statements and detailed rules. General statements are consistent with controls within ISO/IEC 27002 [1] standard. Rules apply to network and systems configuration, user interaction with systems and applications, and detailed processes and procedures (governance, operational teams, and audit). Violation of a rule brings about nonconformity, which is either an incident or vulnerability.

**sensitivity level:** level which corresponds to the potential impact (financial, legal or brand image) of a security event on an asset, an impact linked to the estimated value of the asset for the company along four possible viewpoints: its Confidentiality, Integrity and Availability (CIA) and sometimes its accountability

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

- *Dangerousness* is the result of multiple factors combined together according to circumstances or types of incidents: propagation speed for a worm, virulence, effectiveness, importance and number of impacted assets, capability of harm, target reachability, capability of remote action, persistence, weakness or lack of curative means, and extend of compromise (depth of component which is can be or has been reached, concept of Defence in Depth or DiD).

- *Stealthiness* covers the level to which the incident can be hidden to the defender: obvious visibility, visible through simple and easy to use mechanisms, detection requires advanced technical tools, almost invisibility. It is a key factor for monitoring and detection. Anonymization and camouflage, or active and passive masking techniques are stealthiness techniques. Stealthiness takes on an indirect meaning when it applies to similar not yet detected incidents.

- *Feasibility* describes the attacker's motivation and skills. It increases proportionally to all the necessary prerequisites (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 change. For example, it may be difficult to create a hacking tool for a given vulnerability. However, once the tool is released on the Internet, it can be used by unskilled attackers. Feasibility takes on an indirect meaning when it applies to a potential threat (see definition of this term), as the analysis of its factors required to evaluate it provides an interesting evaluation of the risk.

NOTE: This notion appeared in the mid-1990s within the framework of the ITSEC certification, then towards the end of this decade with the issue of global and public management of vulnerabilities and "malware" (security software vendors and CERTs). It is once again being developed at the present time with the recent release of log analysis and correlation tools that completely integrate this concept along with criticality.

**severity level (of vulnerability or of nonconformity):** The severity level definition is about the same as the one for incidents, with a few small differences:

- *Dangerousness*: impact of the related attacks, weakness of protective techniques, possible remote exploitation, scope of the target/victim population (number of machines, of services, etc.), importance to organization of the security rule that was violated.

- *Stealthiness*: same definition as for incident.

- *Exploitability* (by attackers), is the opposite definition of incident feasibility.

NOTE: The proposed definition is aligned with the CVSS (NIST SP 800-126 [2] or SCAP) standard for software vulnerabilities.

**taxonomy:** science of identifying and naming species, and arranging them into a classification

NOTE: The field of taxonomy, sometimes referred to as "biological taxonomy", revolves around the description and use of taxonomic units, known as taxa (singular taxon). A resulting taxonomy is a particular classification ("the taxonomy of ..."), arranged in a hierarchical structure or classification scheme.

**threat:** potential cause of an unwanted incident, which may result in harm to a system or organization

NOTE: There are 4 categories of threats:

- Natural threats:
  - Environmental causes: public service outage, fire, and other disasters
  - System failure: physical or software computer or network breakdowns

- Human threats:
  - Unintentional (error, carelessness, irresponsibility, unawareness, etc.): conception and design, development, operation and usage, due to chance, hasty development and deployment, tiredness, gullibility, incompetence
  - Internal or external malice: theft, economic spying, sabotage, intrusion, fraud, etc.

The frontier between error, carelessness and malice is often fuzzy: it is always possible for an unscrupulous employee to plead error even though he has been negligent or malicious. However the difference between unintentional and malicious actions can often be found with the following clues:

- An unintentional action is not hidden (so not stealthy), it tends to impact availability rather than confidentiality and integrity, and it has a low dangerousness and a high feasibility. The resulting severity is often low to fairly low.
- A malicious action is stealthier (notably to enable the attacker to remain anonymous and allow him to sustain the advantages obtained for a longer period of time), with an impact on confidentiality and integrity rather than on availability, and with high dangerousness.

**trace:** computer data that proves the existence of a business operation

NOTE: As an example, logs (see definition above) are traces, but traces are not necessarily logs.

**vulnerability:** undesirable state of a system whose occurrence or detection is a security event

NOTE: It corresponds to a flaw or weakness of an asset or group of assets (at the level of a technical system, process or behaviour) that can be exploited by a threat. Occurrence and actual detection of a vulnerability (often delayed in time) are considered the same in the present document. There are 6 types of vulnerabilities, but only the first four are in the scope of a SIEM approach and are being dealt with in the present document:

- Behavioural.
- Software (that can lead to malicious exploitation by an attacker via an "exploit").
- Security equipment or software configuration (same as above).
- General security technical or organizational (vulnerabilities defined as having a global and major effect on Information System's security level, and having a level equivalent to the 133 ISO/IEC 27002 [1] standard control points).
- Conception (overall system design at architecture and processes levels).
- Material level (corresponding with vulnerabilities which enable physical incidents - of an accidental, negligent or malicious kind).

A behavioural, configuration, global security (technical and organizational) or material vulnerability becomes a nonconformity (see definition above) when it violates the organization's security policy and rules. The present document uses the terms "usage or implementation drift" in this case.

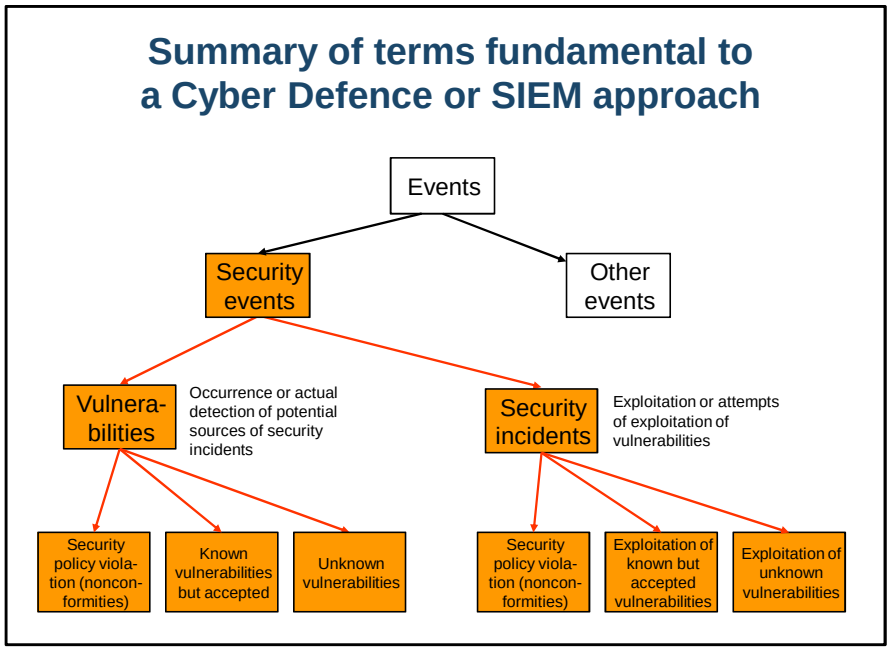


**Figure 2: Relationships between different kinds of events**

## 3.2 Abbreviations

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

| | |
|---|---|
| AD | Active Directory® |
| APT | Advanced Persistent Threat |
| CAG | Consensus Audit Guidelines |
| CAPEC | Common Attack Pattern Enumeration and Classification (Mitre) |
| CCE | Common Configuration Enumeration |
| CEE | Common Event Expression |
| CI | Computer Interface |
| CIA | Confidentiality Integrity Availability |
| CIO | Chief Information Officer |
| CISO | Chief Information Security Officer |
| COA | Courses Of Action |
| CSIRT | Computer Security Incident Response Team |
| CSS | Cross-Site Scripting |
| CVE | Common Vulnerabilities and Exposures |
| CVSS | Common Vulnerability Scoring System |
| CWE | Common Weakness Enumeration |
| CybOX | Cyber Observable eXpression |
| DDoS | Distributed Denial of Service |
| DLP | Data Leak Prevention |
| DNS | Domain Name Server |
| DoS | Denial of Service |
| DPI | Deep Packet Inspection |
| HIDS | Host-based Intrusion Detection System |
| HTTP | HyperText Transfer Protocol |
| IDS | Intrusion Detection System |
| IP | Internet Protocol |
| IPS | Intrusion Prevention System |
| ISM3 | Information Security Management Maturity Model |
| ISMS | Information Security Management System |
| ISO | International Organization for Standardization |
| IT | Information Technology |
| ITIL | Information Technology Infrastructure Library |

| | |
|---|---|
| LDAP | Lightweight Directory Access Protocol |
| MAEC | Malware Attribute Enumeration and Characterization |
| NIDS | Network Intrusion Detection System |
| NIST | National Institute of Standards and Technology (USA) |
| NSA | National Security Agency (USA) |
| OS | Operating System |
| PC | Personal Computer |
| SIEM | Security Information and Event Management |
| SOC | Security Operation Center |
| SOC | Security Operations Centre |
| SQL | Structured Query Language |
| STIX | Structured Threat Information eXpression |
| TTP | Tactics, Techniques and Procedures |
| VDS | Vulnerability Detection System |
| VPN | Virtual Private Network |
| WS | Workstation |
| XML | Extensible Markup Language |

# 4 From basic events and traces to security incidents

The contribution of a SIEM implementation for detection (notably through implementation of powerful tools) consists primarily in unearthing previously undiagnosed security events (in particular those which are very stealthy and lead typically to breach of confidentiality or to a lesser extent to breach of integrity); it also aims at highlighting so-called "weak signals", events that provide advance notice of security breach attempts (scouting, mapping, connection failures, etc.), allowing the organization to deal with these events before more serious consequences occur and to demonstrate a far better reactivity. SIEM implementation for detection is therefore about highlighting potential sequences of events leading up to a security incident (i.e. with actual impact measured by loss of C, I or A on the targeted or concerned asset). Note that these events can typically be detected and qualified shortly after they occur (thus meaning that a potentially new reaction to critical incidents can be quickly triggered by the organization, situation where nothing was happening previously).

Figure 3 summarizes the evolution over time of an attack or misuse event stream when a security incident occurs (applicable mostly to malice and carelessness).

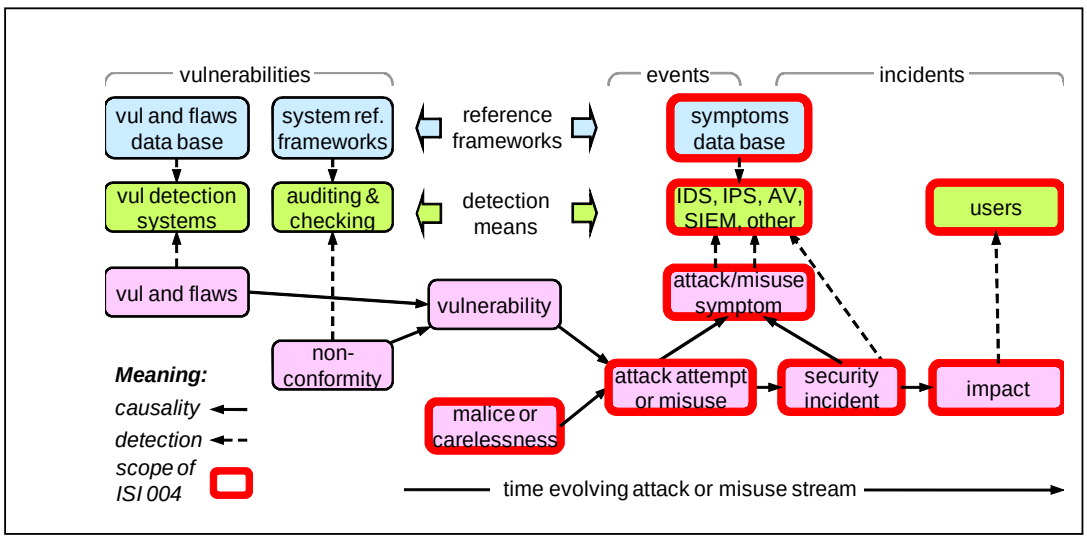


**Figure 3: Positioning of the various elements involved in an attack or misuse**

The first priority is of course to spot the most basic vulnerabilities (being exploited in 70 % of all incidents occurring in real life, as explained in introduction of GS ISI 002 [i.3]), while the remaining security incidents shall be detected by other means. In the case of these incidents (when they are of a malicious nature), the attack stream in figure 3 can be refined in the following 5-step process (using or not social engineering):

1) Fingerprinting, exploration, spying and intelligence gathering (lawful and unlawful information collection).

2) Sabotage (to neutralise or weaken security protections).

3) Intrusion (to get illicit access to the target).

4) Installation of malware and other utilities (to maintain a foothold within the target, and possibly exfiltrate information or launch further actions later).

5) Concealment or camouflage (to conceal attacker's presence, by erasing evidence for example).

Most of the malicious security incidents use only a few steps (typically 1 or 2 steps. Complex ones (such as APTs) encompass all steps. Annex B/clause 1.3 ("How") of the GS ISI 002 [i.3] Event Classification Model describes for each kind of incident listed in clause 1.2 ("What") the main methods and means for an attacker or user to achieve the concerned incident. This description is a 1st input to identify a given incident and to figure out ways to detect it. Such a way for IDS, IPS or Antivirus tools is the definition of a signature of the attacks. But despite huge efforts by tools vendors, this technology has demonstrated clear limits so far notably because of the exploitation of unknown zero-day software vulnerabilities and therefore of rapidly-changing and swift attacks or malwares. An alternative up-and-coming way has been instead to detect the consequences or symptoms (or artifacts) of attacks, as they can be viewed in networks or systems behaviours modifications. The underlying principle is to establish a baseline in the Information System behaviour, and track any deviation from it.

Depending on the step reached by the attack, symptoms (or artifacts) are either advanced signs (or indicators) of an attempt underway or signs (or indicators) of an already successful attack. These symptoms, which can be categorized in various classes, are described in clause 6, together with the principle methods, means and (security, network or system) monitoring tools to detect them.

Even though tools have become significantly advanced and powerful, the analysis and diagnosis of suspicious events by skilled security SOC professionals remains essential since symptoms of attacks are not necessarily caused by actual security incidents. This key human issue is at the heart of security monitoring and is what makes it sometimes so challenging to present tangible results to organisation's executives.

All these difficulties show that it is necessary to implement **both top-down and bottom-up approaches** (see clause 6.5), which combine threat intelligence provided by security governance and measured by state-of-the-art figures (associated to GS ISI 001 indicators) with creative means of detection of related security events as they can be provided by field security experts.

# 5 Positioning the various elements against the MITRE CybOX and STIX reference frameworks

International in scope and free for public use, the Cyber Observable eXpression (CybOX ™) is a standardized schema developed by the MITRE corporation and written in XML for the specification, capture, characterization and communication of events or stateful properties that are observable in the operational domain. A wide variety of cyber security use cases rely on such information including: event management/logging, malware characterization, intrusion detection, incident response/management, attack pattern characterization, etc. CybOX provides a common and flexible mechanism (structure and content) for addressing cyber observables across and among this full range of use cases improving consistency, efficiency, interoperability and overall situational awareness.

The Structured Threat Information eXpression (STIX™) is a collaborative community-driven effort led by the MITRE corporation to define and develop a standardized language to represent structured cyber threat information and enable easier and quicker information sharing among concerned stakeholders. The STIX Language intends to convey the full range of potential cyber threat information and strives to be fully expressive, flexible, extensible, automatable, and as human-readable as possible. In addition, STIX provides a unifying architecture tying together a diverse set of cyber threat information (with relevant MITRE standards indicated) including:

- Cyber Observables (CybOX), which are the "base" element within the STIX structure (for example, information about a file, a registry key value, a service being started, an HTTP request being sent - see also CEE).
- Cyber Threat Indicators, which are a construct used to convey specific Observables combined with contextual information intended to represent artifacts and/or behaviours of interest within a security context (Let us note that Indicator has here a different meaning as in GS ISI 001).
- Security incidents (see CAPEC and MAEC).
- Adversary Tactics, Techniques, and Procedures (including attack patterns, malware, exploits, kill chains, tools, infrastructure, targeting, etc. - see CAPEC and MAEC), which are representations of the behaviour or modus operandi of cyber-adversaries.
- Exploit Targets (e.g. vulnerabilities or weaknesses in software, systems or configurations - see CVE, CWE and CCE), that are targeted for exploitation by the TTP of a Threat Actor.
- Courses of Action (COA), e.g. incident response or vulnerability/weakness remedies, which are specific measures to be taken to address threat whether they are corrective or preventative to address Exploit Targets, or responsive to counter or mitigate the potential impacts of Security incidents.
- Cyber Attack Campaigns, which are instances of Threat Actors pursuing an intent, as observed through sets of incidents and/or TTP, potentially across organizations.
- Cyber Threat Actors, which are characterizations of malicious actors (or adversaries) representing a cyber attack threat including presumed intent and historically observed behaviour.

Interest in presenting STIX and CybOX in the present document is motivated by its extended scope, ranging from IT non-security information to high-level IT security events, making it possible to further position the various elements introduced in figure 3 of clause 4. Figure 4 describes this mapping with STIX and CybOX elements.

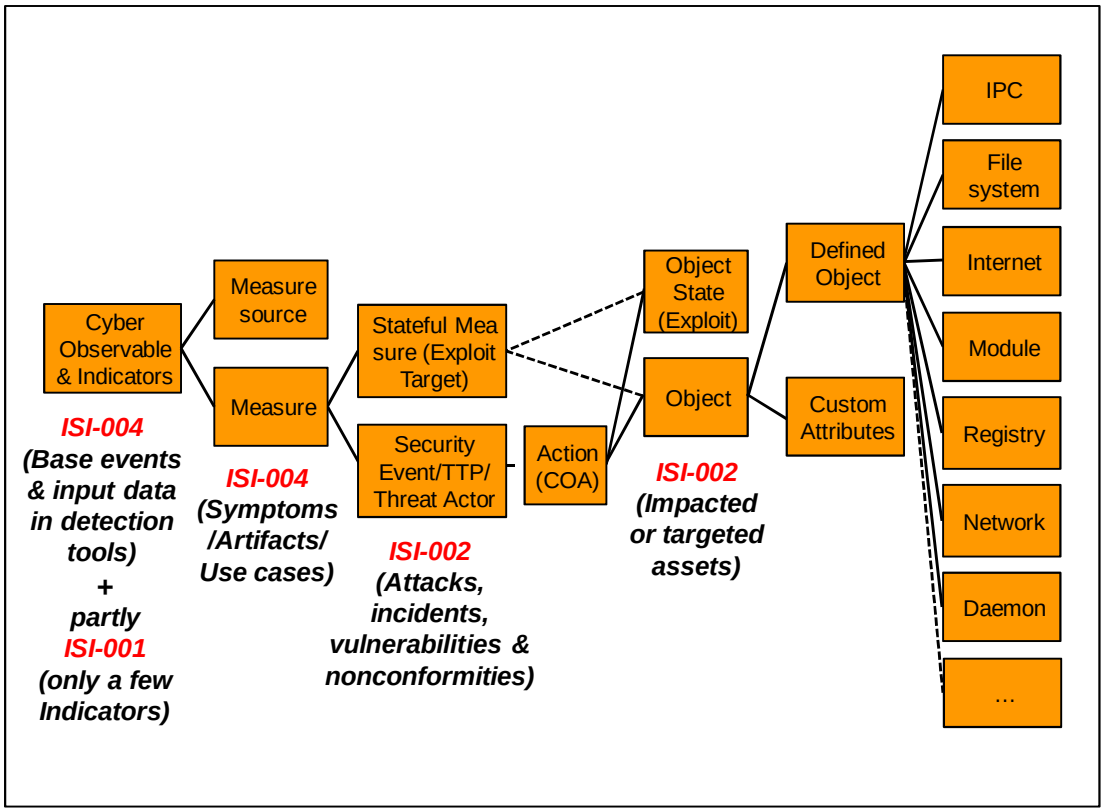


**Figure 4: Mapping of STIX and CybOX elements with GS ISI multi-part series concepts**

# 6 List of symptoms/artifacts and methods of detection

## 6.1 Symptoms/artifacts/hints

The symptoms, artifacts and hints that lead to the detection of security events can be categorized in **3 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 elaborate correlation (especially known structured and complex attack patterns).

The **1st category** consists in establishing a baseline of usual or acceptable behavior and in detecting deviations. The principal method for implementing anomaly detection relies on the use of statistical techniques and machine learning to create a reference model. Examples of monitored information include:

- at the network level, flow size (for example, usual size of flows for each internal host), communication direction, service request rate (for example DNS), communication patterns (for example internal hosts connecting to many other internal hosts);
- at the system or application level, list of processes, loads (especially during off-peak or weekend hours), communication streams direction, access rate to some resources and applications, access rate to some actions, activity of accounts, rate of rejections to some resources;
- regarding log information, log data string size (suspicious if too bulky), log data timeliness (suspicious if limited interruption);

- regarding user behaviours on workstations or central systems, identities and credentials (brute force, account sharing, theft of credentials, failed authentication), user connection profiles (time and frequency), data protocol usage, mail usage, files download, dump of data bases, file access methods (through some suspicious resources), suspicious extension of rights or escalation of privileges;
- integrity of files (especially key files and files content changes).

The **2nd category** consists in detecting well-characterized attack patterns, and also exploits or methods of exploitation of known conception or software or configuration vulnerabilities. The main method for detecting such attack patterns is through the definition of signatures (for example regular expressions). Examples of misuse that can be detected through such methods include:

- malware installation;
- intrusion attempt such as SQL injection (entry of unusual string of characters into a Web application);
- Attempt to use a forbidden set of commands in an application;
- Commands stemming from hosts with origin addresses with a unusual or erroneous structure or without a standard known structure;
- Attempts to access non-existent resources (through the use of honeypots).

This detection method applies to public software vulnerabilities (CVE tagged), to widespread application software programming errors (CWE tagged) such as lack of control of data entries for example, and to common weaknesses in products configurations against standard security policies (CCE tagged).

Another slightly different detection method in this category consists in identifying internal hosts appearing to be compromised or to be under attack by detecting known rogue URLs (from e-reputation lists for example).

The **3rd category** consists in detecting known structured and complex attack patterns (with well-characterized scenarios) or security events requiring correlation of several more basic events. It comprises generally combination of events of the other categories, and consists often in an attack stream that can be split in a 5-step process (fully or partly). Some examples of cases are the following:

- Web intrusion;
- Advanced Persistent Threat (APT);
- physical and logical consistency between user's physical situation and his interaction with the information system;
- access control at the server or network levels (for example, back-door detected by comparison of the number of IP entries and the number of OS threads on an application, or external access to internal resources by outbound tunnelling detected by outbound links, or access to Internet through an anonymization Website);
- logs integrity (for example, suspicious log data string operations interruption when correlated to server intrusion).

The **1st category** is the only one among all 3 to focus on the detection of consequences of a security incident, the 2 other ones detecting rather direct hints of security events. For this reason, a significant qualification period is required to identify and categorize the event itself. The strength of this method is its applicability to all kinds of attack processes and its genericity (not depending on prior knowledge of signatures of given attacks or behaviours). Its weakness is the difficulty to spot very faint deviations against the baseline. In this category, the challenge is to spot a "needle in a haystack".

The **2nd category** is the most straightforward way to detect attack patterns, since it reuses the knowledge of precise features about attacks or incidents and/or on existing vulnerabilities whose existence and exploitation is necessary to carry out the related incidents. Its strength is an efficient and reliable technique to detect well-defined incidents (through well-defined signatures) and is always effective and efficient for well-established common weaknesses (programming errors and configuration nonconformities). Its weakness relies in its impossibility to detect unknown and rapidly-changing attack patterns or software vulnerabilities (such as zero-day ones). In practice, an additional weakness is the impact of the detection algorithm on the monitored system or the hosting sensor (memory or bandwidth requirements, introduction of latency and jitter in the network traffic, capability offered to the attacker to hide the information under multiple layers, etc.).

The **3rd category** is the most "creative" and complex one, since it is necessary to imagine as many ways as possible that perpetrators will use to carry out the assumed security incidents. The strength of this method is a secure way to detect well-defined incidents, its weakness being its impossibility to figure out all the possible cases and the possible complexity in detecting some identified cases.

As mentioned in clause 4, an attack stream can be split in a 5-step process, each step often requiring a dedicated and different way of detection. Detecting very stealthy security incidents may require the use of several categories of artifacts or hints, especially the combination of category 1 (of a somewhat different nature as mentioned above) and one of the 2 other categories.

As a result, detection of complex security incidents (such as APTs for example) which comprise the 5 steps may require the use of indicators belonging to all the categories, therefore maximizing the chance to spot them (see the example in clause 7.2).

## 6.2 Which relevant categories for each incident field (regarding its characteristics)

The prerequisite of detection is often to know what to detect. As stated earlier in the present document, the detection is based on detection of symptoms. The symptoms of an incident are closely linked to its characteristics.

The GS ISI 002 [i.3] document defines what an incident is and defines the characteristics of incidents using the following attributes:

- Its origin ("Who & Why")
- The action performed ("What")
- The technique used ("How")
- Its status
- The vulnerability exploited
- The impacted target ("on what asset")
- CIA consequences
- Business consequences ("Kind of impact")

### 6.2.1 Symptoms linked to the incident origin

The detection of such symptoms does not necessarily mean the existence of incidents. It only indicates that initial conditions for an incident are present. The effective existence of the incident has to be confirmed by the detection of other symptoms. Only few symptoms are obvious to detect, such as occurrence of natural disasters. The other symptoms (errors, carelessness, malice) are related to personal behavior, and their detection would require the implementation of personal profiling techniques. Misuse detection techniques could be the most efficient ones for detection of natural disasters. It requires the specification of dangerous events (earthquake, storms, floods, abnormal temperature, etc.). Personal profiling techniques could rely on both misuse detection and anomaly detection.

### 6.2.2 Symptoms linked to actions

Symptoms linked to actions are key symptoms because the detection of such symptoms (illicit access to system, unauthorized action, system disturbance, etc.) provides a high level of certainty of the presence of an incident. Such symptoms would not need to be confirmed by other symptoms but consistency checks with other symptoms could be useful before implementing a response. Examples of symptoms linked to the action performed are: the unavailability of a service due to a denial of service attack, abnormal negative feedbacks from customers, disturbance of regular operations, abnormal use, absence of employees, etc. Both misuse detection and anomaly detection techniques could be used. And let us add that analysis worked out in clause 6.1 applies fully here.

### 6.2.3 Symptoms linked to techniques used

It is impossible to define generic types of symptoms for the "technique used" characteristics. The symptoms are specific to each technique: for example, transactions replay, presence of malware, use of account out of normal service hours, etc. Misuse detection techniques may sometimes provide a higher level of assurance of the existence of an incident. Anomaly detection techniques can also be implemented but give lower level of assurance than the previous method. And let us add that analysis worked out in clause 6.1 also applies fully here.

### 6.2.4 Symptoms linked to vulnerability exploited

The only symptoms linked to the "vulnerability exploited" characteristics are the presence of the vulnerability in the system while the system is attacked. Vulnerability detection techniques apply here as a component of misuse detection techniques (notably through the coupling of VDS with IDS or IPS). Efficiency rates are specific for each type of vulnerability detection and incident detection techniques.

### 6.2.5 Symptoms linked to the incident status

The status of an incident is hard to define before the actual detection of the incident. It depends on the final objective of the incident. Additional investigations are required after the suspicion or the actual detection of an incident. No symptoms can be specified here.

### 6.2.6 Symptoms linked to assets and CIA consequences

Symptoms linked to the targeted asset and the CIA consequences have to be analyzed together. A classic symptom is the presence of abnormal elements in the targeted asset, such as abnormal change of the assets binaries, of the asset configuration or of the asset behavior. The detection of such symptoms could be misleading because an asset corruption could be either the final result of the incident or only an intermediate step towards another final asset. For example, additional investigations are required in case of detection of disturbance of a security device. That disturbance could be only a step for camouflage of an on-going attack. We should also add that the CIA sensitivity of the asset and the type of hosted information may be key indicators to determine whether or not it is an interesting final target for attackers. Both misuse detection and anomaly detection techniques could be used.

### 6.2.7 Symptoms linked to business consequences

The detection of symptoms related to business consequences could be applicable but practically it could be very hard to decide if an abnormal business situation (loss of productivity, reputation damage, loss of market share, etc.) is caused by a security incident or not. Both misuse detection and anomaly detection techniques could be used.

### 6.2.8 Summary

Table 1 summarizes the analysis of applicability of detection techniques (limited to categories 1 and 2) to symptoms linked to the 8 incident attributes. Sometimes category 3 may help in qualifying an incident; for example, when it is about the origin and if an internal user is concerned, it may be necessary to correlate a suspicious behaviour with other information such as the employment situation (recently sacked, deeply disappointed, etc.).

**Table 1: Applicability of detection techniques**

| Incident fields (characteristics) | Detection techniques | |
|---|---|---|
| | Anomaly detection (category 1) | Misuse detection (category 2) |
| **Origin** | Applicable but confirmation by other symptoms is required | Applicable but confirmation by other symptoms is required |
| **Action** | Applicable (efficiency depends on the type of action) | Applicable (efficiency depends on the type of action) |
| **Technique used** | Applicable (with lower level of assurance than category 2) | Applicable (with sometimes high level of assurance) |
| **Exploited vulnerability** | Not applicable | Applicable (efficiency depends on the type of vulnerability detection and associated incident detection techniques) |
| **Status** | Not applicable | Not applicable |
| **Targeted asset & CIA consequences** | Applicable (but additional investigations required) | Applicable (but additional investigations required) |
| **Business consequences** | Applicable (but with low efficiency) | Applicable (but with low efficiency) |

## 6.3 Which relevant categories for each step of the 5-step attack stream

It may be interesting at that stage to tentatively map in a generic approach the different categories with each step of the 5-step attack stream introduced in clause 4. Table 2 is an attempt to show the feasibility and usefulness of such an approach.

**Table 2: Which categories for each step of the 5-step attack stream**

| Steps / Hints/ Symptoms | 1 (Exploration and spying) | 2 (Sabotage) | 3 (Intrusion) | 4 (Malware and utilities installation) | 5 (Camouflage) |
|---|---|---|---|---|---|
| **Category 1** | X | X | X | X | X |
| **Category 2** | | | X | X | |
| **Category 3** | X | | X | X | X |

In the 1st step and if we exclude lawful information gathering (often difficult to detect), the attack is characterized by an unlawful search for possibly useful and later exploitable information, through more or less stealthy methods. Unlawful methods include passive ones such as wiretapping, data copying or directory access, or active ones such as systematic network reconnaissance, social engineering based (for example phishing), material theft or diversion of data flow. Depending on the active method used, category 1 may be useful (intensive reconnaissance for example with clear deviation against the usual network behaviour) or category 3 may be preferred in the case of other well-defined scenarios including strong interaction with the information system.

In the 2nd step, the attack methods are almost always visible and active, and therefore detectable. The objective being to weaken or neutralise defences or sometimes to distract organisation's IT security teams' attention, the attacker seeks to create deviations from normal operations, which means category 1 is the right candidate to discover these attacks. The methods used include DoS or DDoS attacks, logic bomb, physical destruction, security control or access control deactivation.

In the 3rd step, the attack methods are very diverse, ranging from very stealthy to more obvious ones. So all categories may be concerned. Stealthy attack methods include user impersonation, access control diversion, software vulnerability exploitation. Obvious attack methods include authentication brute force attacks on access control systems, extension of privileges or intrusion on a user's workstation (further to spear-phishing tactics that let him carry out a dangerous action). These methods may in some cases follow a physical intrusion.

In the 4th step, the methods of attack are similar to the third step and consist in installing (locally or remotely) on the host malicious software or utilities by exploiting legitimate accesses, software vulnerabilities and/or configuration vulnerabilities; the objective is to get a foothold on the host in order to be able to come back later as often as necessary (inbound or outbound back-door, with or without an illicit account), and to possibly penetrate deeper into the internal network. The relevant methods of detection are categories 2 and 3. Category 1 may also be involved afterwards when the malware is a bot communicating with a botmaster and exfiltrating information.

In the 5th step, the methods used are generally to erase logging features of the host or traces of the attacker's activity (especially logs); it is also about remaining as long as possible "under the radar" by hiding the malware (rootkit features) or limiting dramatically its activity or by communicating with the external Internet world as little as possible or through data encryption. Due to this objective of camouflage, detection may be difficult, but log stopping is a relevant symptom that can be closely monitored (category 1) and an example of category 3 implementation is detection of encryption of data exchanges with the Internet originating from a workstation on the organization's internal network.

## 6.4 Which methods of detection and tools should be used

Table 3 is a mapping between the main categories of hints/symptoms and the tools required to support and enable detection (sensors/point devices/information forwarders and processing/correlation units). DLP (Data Leak Prevention) tools are not included in this analysis since they are effective only in cases of user carelessness or plain error (which scope is not the main goal of the present GS). VDS tools, which are very useful as inputs to SIEM platforms or as complements to IDS, are also not included in this analysis since they address vulnerability and/or nonconformity detection (out of the scope of the present GS).

**Table 3: Which possible detection tools for each category**

| Tools / Hints/ Symptoms | Network management | System management | Integrity checking | HIDS | NIDS and DPI | Anti-malware | SIEM correlation tool |
|---|---|---|---|---|---|---|---|
| **Category 1** | X | X | X | X | X | | X |
| **Category 2** | | | | X | X | X | X |
| **Category 3** | X | X | | X | X | X | X |

The **1st category** requires data both from network and system management (such as size of flows and streams) and from network/system/application logs (to work out usual user profiles), to enable SIEM tools to detect values crossing thresholds. Some IDS tools can also provide network behavioural data, monitoring and alerting on possible abnormal changes in network traffic patterns (idem for HIDS at application/system/OS levels - Cf. often the best suited tool to detect generic abuse or escalation of privileges). And integrity checking tools can on an almost continuous basis detect possibly abnormal changes in files content (if coupled to change management tools). Asset management tools (which are a desirable complement of all detection tools in Security Operations Centers) give a comprehensive picture of the whole information system, whose mapping is deemed mandatory to avoid unknown holes in the cyberdefence scheme; for we shall keep in mind that some studies or surveys have shown that up to 70 % of all security incidents exploit unknown and/or unmanaged (and therefore vulnerable) assets. This is due to the fact that more than 95 % of all attacks are opportunistic and are first looking for weak and vulnerable systems regardless of specific organizations or targets.

The **2nd category** relies on dedicated tools (mainly IDS at network level) to spot detailed signatures of attacks through recognition of precise hints or exploits. Another monitoring technique is detection at application and system level through HIDS. Moreover, SIEM tools can help filtering false positives (some SIEM systems being dedicated to that and effective achieving that). And through other categories and alternative means, they can also help in detecting false negatives, and therefore improving the data base of detection rules in IDS. The SIEM capabilities can also be used to compare all inbound or outbound addresses with lists of rogue URLs.

The **3rd category** requires a wider range of diversified tools, depending on the complexity of attacks and scenarios that shall be detected. IDS, HIDS and DPI tools try to detect known attack signatures (more or less dedicated and specific to given attacks), Antivirus and antimalware are the oldest and most vintage way of detecting mainstream malware through signatures of known malicious software (and in spite of their more and more frequent relative effectiveness, probably still thwarting more than 90 % of all of them). System management provide specific information that is not available in logs, such as active threads and processes on an application or some active dangerous administrative sub-systems. Asset management tools may also be necessary, but for a somewhat different reason as the one mentioned previously; they enable to obtain a clear mapping of the various components in the information system and therefore of the possible alternative routes towards targets for attackers. And SIEM tools do the same job as for all other categories, i.e. bring together various hints stemming from network/system/application logs and other previously mentioned tools.

Very dedicated tools may also be used here especially to detect very stealthy attack; it is about network probes (some of them being developed and implemented by government security agencies, with advanced detection rules of IDS-based engines); they try to overcome classical shortcomings of IDS and DPI tools. Some SIEM tools also complement and improve their log-based analysis by collecting further information from complementary probes (using protocols such as NetFlow).

Another additional technique to help detect security incidents is the use of intelligent display through original, advanced and often 3D graphic visualization. Examples of methods that enables to both recognize and better understand attacks are (overall situation or drill-down on suspicious incidents):

- Monitoring unused and rogue IP addresses (so-called darknets) and active IP addresses within the organization attempting to send packets to an address in the darknet, and displaying this data through 3D globes representing the Internet and various networks under observation, and alerting operators through a colour change when an unused address is hooked up.
- Visualizing all IP links for a given application or process on a host (whether central system or workstation), providing a new and interesting connection to understand the process or application behaviour and to help identify more quickly something unusual and possibly malicious and the source of attack and of compromise (typically a bot discussing with a command and control center).
- Using a cube (3-dimension space, i.e. source x destination x service) to display all internal and external connections.

## 6.5 The key role of seasoned experts in detection

The previous clause describes the contribution and role of the different categories of tools in security event detection. It shows in particular the correlation role of SIEM tools (against the more specific role of all other tools) to detect many security events. However, the power of the technology is still often limited in such a difficult area with so stealthy attacks. The often weak signals which are able to reveal underway attacks are generally hidden in huge amounts of data and/or in some unusual places. In this context, the role of SOC operators and experts remain essential and their experience is key. And the various visualization means as mentioned in the previous clause are of great importance to help them spot these signals and make a diagnosis. These means together with human experience enable to display more prominently unusual behaviours as regards the information system various components.

It should be added that complementing hands-on experience of SOC personnel by training sessions and relevant tools is highly recommended. Training tools simulating cyber situations and attacks (kind of "war games") will be more and more required to develop cyber skills.

## 6.6 The key role of threat intelligence and associated process

As a result of the above-mentioned difficulties, threat intelligence and knowledge is becoming of utmost importance. It brings valuable clues about where to search for likely security events, giving you the best chances to spot existing needles in the haystack. Let us take an example with an external intrusion on the organisation's internal network; there are 7 main ways to carry out such an attack (by descending order of likelihood):

- Through a malware installed on a workstation (mainly via spear phishing), then access to the internal network followed by illicit access to internal servers.
- Physical intrusion (followed by logical access).
- Through a firewall (with social engineering).
- Stolen and ill-protected user's laptop (and use of VPN access).
- Ill-protected wireless network.
- Identity usurpation on an Extranet (and privilege escalation).
- Exploitation of an outbound Internet link set up by an internal user (from their PC).

In this example, we can see how diversified the means are to enter into the organisation's information system, with as many diversified detection means. Beyond this 1st level of knowledge, it is important to get a clear idea about the proportions of each of them, and therefore to prioritize targets of detection. This is what has been called a top-down approach to detection, where the key role of **threat intelligence** steps in and where GS ISI 001-1 [i.1] indicators together with their state-of-the-art figures are so required.

To implement such a top-down approach and combine it with a bottom-up approach consisting in detection tools/methods/use cases engineering (resting especially on SOC experts creativity), it is key to implement **dedicated processes** (which can be called **"Use case definition"**), which can be derived from the usual ITIL change and release management processes. The goal is to make sure that the security governance and the SOC experts and managers meet periodically to talk about security event detection improvement (scope of detection and effectiveness of existing means); the stake is to challenge SOC capabilities to come closer to the reality as regards attacks and deviant behaviours. Since the current situation about detection is still very poor, leading within organizations to disappointment and low RoI (Return on Investment), this is an effective way to get steady and continuous progress in this matter. This way of proceeding is also the opportunity to establish a direct link with IT risks and general enterprise governance frameworks (see GS ISI 001-2 [i.2]), demonstrating more added value brought by the whole detection scheme and generating more trust in the organisation's ability to better know IT residual risks it faces.

# 7 Examples to illustrate the previous concepts

It would be too tedious and far too complex to build a comprehensive link between GS ISI 002 [i.3] security event classification model and the present document symptoms and artifacts classification, but illustration through 2 wide-spread special incidents will enable to cover a wide range of categories of hints and symptoms. The 1st security incident described below (Internet-facing Web application intrusion) is one of the most frequent security incidents organizations face today, the 2nd one (Advanced Persistent Threat) being one of the most dangerous ones while being often very difficult to detect.

## 7.1 Internet-facing Web application intrusion

In the GS ISI 002 event model [i.3], this incident is tagged as **IEX_INT.2** (or possibly **IEX_UID.1**), and the detailed associated taxonomy enables to clarify it and characterize it more dependably (see table 4). And as regards its position in the 5-step attack stream model, it concerns only step 3 (Intrusion).

**Table 4: Taxonomy for Internet-facing Web application intrusion**

| Who and/or Why | What | How | Status | With what vulnerability(ies) exploited | On what kind of asset | With what CIA consequences | With what kind of impact |
|---|---|---|---|---|---|---|---|
| Malicious act/External agent | 2 choices (see note 1) | Many possibilities (see note 2) | Incident success | Many possibilities (all kinds of vulnerabilities) | 1 choice (see note 3) | All possibilities (CIA) | - |

NOTE 1: Technical intrusion on a central system or an application, use of authorized user's identity (identity usurpation or user impersonation) without identity owner's consent and agreement.

NOTE 2: For technical intrusions, various methods:
- Command execution/injection attack (OS commanding, LDAP/SQL/XML/e-mail command/... injection, buffer overflow, format string, other)
- Usurpation of functionality (path or directory traversal, cache poisoning, etc.)
- Protocol manipulation (special unusual commands, HTTP request/response smuggling/splitting)
- Client-side attacks through malware installation (cross-site scripting CSS, man-in-the-browser or man-in-the-middle attacks for theft of cookies)
- Miscellaneous

For authentication attacks, different methods:
- Brute force
- Exploitation of poor credentials (easy to guess)
- Lack of authentication (i.e. no login)
- Use of stolen credentials

NOTE 3: Data bases and applications**/**Perimeter**/**Web (bespoke or not) application.
With such a detailed characterization and identification, it is possible to list the various known methods of attacks to figure out the best way in each case to detect the incident by devising which hints/symptoms/artifacts may be present. Technical intrusions and identity usurpation, which are very different, shall be addressed separately.

### *Technical intrusions*

We shall consider each main known method (see note 2 above) and try to find out the simplest hints/symptoms/artifacts for each of them and if possible shared ones. Table 5 lists the various possible cases with a scoring scheme scaling from - (not applicable) to 4 (very efficient). This scheme takes into account both the effectiveness of the detection means and the cost of the required monitoring tools, and therefore measures the efficiency of the method used.

**Table 5: Which relevant category for each method of attack (Technical intrusions)**

| Symptom / Method | Category 1 | Category 2 | Category 3 |
|---|---|---|---|
| Command execution/ injection attack | 3 | 3 | 2 |
| Usurpation of functionality | 3 | - | - |
| Protocol manipulation | 4 | 1 | 2 |
| Client-side attacks through malware installation | 3 | 3 | 3 |

To make it simple (which is almost mandatory in detection), category 1 (through different measures, namely log data string size and files integrity) applies to all attack patterns with a high level of effectiveness. Therefore, there no special need to resort to other categories, which are also often more complex to implement.

### *Identity usurpation*

According to the same process as above, table 6 lists the various possible cases with a scoring scheme scaling from - (not applicable) to 4 (very efficient).

**Table 6: Which relevant category for each method of attack (Identity usurpation)**

| Symptom / Method | Category 1 | Category 2 | Category 3 |
|---|---|---|---|
| Brute force | 3 | - | 4 |
| Exploitation of poor credentials | 1 | - | 3 |
| Lack of authentication | 4 | - | 3 |
| Use of stolen credentials | 2 | - | - |

To make it again simple, category 1 applies to all attack patterns, with varying effectiveness. On the opposite side, category 3 applies to three attack patterns, with high efficiency but with as many different use cases. Selecting one category of symptoms (rather than the other one) depends mainly on the incident criticality, which is related to the sensitivity of targeted assets, either directly and indirectly. Availability of the relevant tools (see clause 6.3) is of course another criteria to select the right scenario. Category 1 requires more common tools than category 3.

## 7.2 Advanced Persistent Threat (APT)

As explained in GS ISI 002 [i.3], clause 4.5, an Advanced Persistent Threat (APT) is a complex incident, that can be broken down in more basic security incidents (see figure 5, with incidents represented by squares and vulnerabilities exploited by circles).

For the purpose of the present analysis, each basic incident (which has its own features) shall be considered separately; the basic incidents to be addressed are the following: possible spear-phishing targeting specific users with spoofed emails (1), malware installed on a workstation (2), attempt to access to an internal server (3), malware installed on a server (4). It is supposed that at least the first and second steps of the attack have been successful (malware installed).

And in the 5-step attack stream mode l, it applies only to step 3 (Intrusion) and step 4 (Malware and utilities installation). The initial step 1 (Exploration), where attackers research and identify individuals they will target in the attacks, using public search or other methods, and get their email addresses, is not taken into account here. And to simplify, step 5 (Camouflage), which is used to maintain persistence within the organization's network, is also not taken into account.

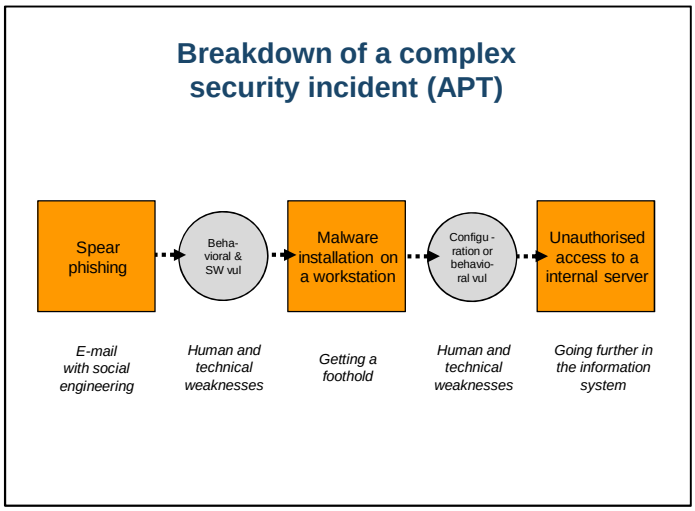


**Figure 5: Description of a complex security incident**

In the GS ISI 002 event model [i.3], the **1st basic incident** is tagged as **IEX_PHI.2**, and the detailed associated taxonomy enables to clarify it and characterize it more accurately (see table 7).

**Table 7: Taxonomy for APT (Spear-phishing step)**

| Who and/or Why | What | How | Status | With what vulnerability(ies) exploited | On what kind of asset | With what CIA consequences | With what kind of impact |
|---|---|---|---|---|---|---|---|
| Malicious act/External agent | 1 choice (see note 1) | 1 choice (see note 2) | Incident success (attached document opened) | Behavioral vulnerability | 3 choices (see note 3) | 1 main possibility (I) | - |

NOTE 1: Reception of a customized and spoofed e-mail impersonating a known authority or usual business relation to entice the recipient to do something harmful to his/her organization (opening an attached document in this case).
NOTE 2: Idem note 1.
NOTE 3: People (with 3 choices):
- Employee
- Business partner
- On-premises or off-premises service provider.

In the GS ISI 002 event model [i.3], the **2nd basic incident** is tagged as **IEX_MLW.3**, and the detailed associated taxonomy enables to clarify it and characterize it more accurately (see table 8).

**Table 8: Taxonomy for APT (WS malware step)**

| Who and/or Why | What | How | Status | With what vulnerability(ies) exploited | On what kind of asset | With what CIA consequences | With what kind of impact |
|---|---|---|---|---|---|---|---|
| Malicious act/External agent | 1 choice (see note 1) | 1 choice (see note 2) | Incident success | Many possibilities (all kinds of vulnerabilities) | 2 choices (see note 3) | 2 main possibilities (CI) | - |

NOTE 1: Trojan horse or back-door.
NOTE 2: One method of installation used: opening a malware-loaded attachment (for example Office or pdf document) in an e-mail message.
NOTE 3: End-user devices (with 2 non-exclusive choices):
- Local application software (user or organization-owned)
- Multipurpose workstations (user or organization-owned).

In the GS ISI 002 event model [i.3], the **3rd basic incident** is tagged as **IEX_UID.1** (with a possible complement tagged **IEX_RGH.1**), and the detailed associated taxonomy enables to clarify it and characterize it more dependably (see table 9).

**Table 9: Taxonomy for APT (Identity and/or right usurpation step)**

| Who and/or Why | What | How | Status | With what vulnerability(ies) exploited | On what kind of asset | With what CIA consequences | With what kind of impact |
|---|---|---|---|---|---|---|---|
| Malicious act/External agent | 2 choices (see note 1) | 2 choices (see note 2) | Incident success | Many possibilities (all kinds of vulnerabilities) | 2 choices (see note 3) | 2 main possibilities (CI) | - |

NOTE 1: 2 non exclusive choices:
- Use of authorized user's identity (identity usurpation or user impersonation) without identity owner's consent and agreement
- Usurpation of rights (privilege escalation)

NOTE 2: For authentication attacks, different methods (especially administrator credentials targeted):
- Brute force
- Exploitation of poor credentials (easy to guess)
- Lack of authentication (i.e. no login)
- Use of stolen credentials

For Usurpation of rights (privilege escalation):
- Brute force attack on root (Unix-like® systems) and possibly further compromission of other servers
- Exploitation of flaws to trigger buffer overflow and generate privilege escalation
- Access through a compromised workstation to other one with full administrative privileges via a Windows® "pass-the-hash" program to finally get shell access on the domain controller
- Miscellaneous

NOTE 3: 2 choices:
- Systems/Internal/Server (Windows®, Unix-like®, other) or Web server or Directory server (LDAP, AD, etc.)
- End-user devices (Local application software or multipurpose workstations).

In the GS ISI 002 event model [i.3], the **4th basic incident** is tagged as **IEX_MLW.4**, and the detailed associated taxonomy enables to clarify it and characterize it more accurately (see table 10).

**Table 10: Taxonomy for APT (Server malware step)**

| Who and/or Why | What | How | Status | With what vulnerability(ies) exploited | On what kind of asset | With what CIA consequences | With what kind of impact |
|---|---|---|---|---|---|---|---|
| Malicious act/External agent | 1 choice (see note 1) | 1 choice (see note 2) | Incident success | Many possibilities (all kinds of vulnerabilities) | 2 choices (see note 3) | 2 main possibilities (CI) | - |

NOTE 1: Trojan horse or back-door.
NOTE 2: One method of installation (malware planted on a server after an intrusion).
NOTE 3: 2 choices:
- Systems/Internal/Server (Windows®, Unix-like®, other)
- Data bases and applications/Internal or outsourcing.

With such a detailed characterization and identification, it is possible to list the various known methods of attacks to figure out the best way in each case to detect the incident by devising which hints/symptoms/artifacts may be present. Each basic incident (among the 4 above-mentioned ones, which are very different), shall be addressed separately.

### *1st basic incident (IEX_PHI.2)*

We shall consider each main known method (see note 2 above) and try to find out the simplest hints/symptoms/artifacts for each of them and if possible shared ones (only one method to be considered here). Table 11 lists the various possible cases with a scoring scheme scaling from - (not applicable) to 4 (very efficient).

**Table 11: Which relevant category for each method of attack (APT Spear-phishing step)**

| Symptom / Method | Category 1 | Category 2 | Category 3 |
|---|---|---|---|
| Spoofed and customized email (with rogue attachment) | - | 3 | - |

To make it again simple, the only applicable category is the 2nd one through the detection of the rogue attachment, with a satisfying level of effectiveness in the case of non zero day vulnerability exploited. Another possible method of detection could be the user himself (and it works sometimes), if he is sufficiently aware.

### *2nd basic incident (IEX_MLW.3)*

According to the same process as above, table 12 lists the various possible cases with a scoring scheme scaling from - (not applicable) to 4 (very efficient).

**Table 12: Which relevant category for each method of attack (APT WS malware step)**

| Symptom / Method | Category 1 | Category 2 | Category 3 |
|---|---|---|---|
| Installation of malware on a workstation | - | 3 | - |
| Malware com-municating with the Internet | 2 or 3 | - | 1 |

2 categories (1 and 2) are applicable, the 1st one once the malware is installed and is in operations and the 2nd one when it is being installed. However, we shall keep in mind that this kind of malware used on targeted attacks is generally very stealthy with the possible exploitation of zero-day software vulnerabilities; it means that both methods of detection require a lot of tuning and often advanced ways of characterization (for either IDS tools or deviations against a base line). But provided that programming is advanced enough (as sometimes government information security agencies teams do it), the best tool remains IDS at network entry.

### *3rd basic incident (IEX_UID.1 and possibly IEX_RGH.1)*

According to the same process as above, table 13 lists the various possible cases with a scoring scheme scaling from - (not applicable) to 4 (very efficient). For IEX_UID.1, see clause 7.1. Only IEX_RGH.1 is addressed below.

**Table 13: Which relevant category for each method of attack (APT identity and/or right usurpation step)**

| Symptom / Method | Category 1 | Category 2 | Category 3 |
|---|---|---|---|
| Compromission of a server following root access on another one (Unix-like® systems) | 1 | - | 2 |
| Buffer overflow triggering and privilege escalation in a WS | - | 1 | 2 |
| Use of "pass-the-hash" program to get shell access to the Windows® domain controller (lateral movement) | - | 1 | 1 |

To summarize, these various methods of getting more privileges on the victim's network to further get access to the targeted sensitive servers are most of the time very difficult to detect with usual tools; HIDS on servers or workstations classified in category 2 would be the best mean, but they are unfortunately rarely available on most hosts. Detecting the attacker's systematic search of interesting hosts on the network (closer to IEX_UID.1 and brute forcing and valid passwords guessing) to access more and more systems is generally easier than this further step.

### *4th basic incident (IEX_MLW.4)*

The analysis is similar to that of the 2nd basic incident, with a possible difference regarding the use of category 1, which may detect deviations in the server workload (usual when downloading or funnelling huge amount of data to staging servers to encrypt and compress them before sending them outside).

# Annex A (informative): Authors & contributors

The following people have contributed to this specification:

**Rapporteur**:
Gerard Gaudin, G²C, Chairman of ISG ISI

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

Federic Martinez, Alcatel-Lucent, Secretary of ISG ISI

*And in alphabetical order:*

Christophe Blad, Oppida

Eric Caprioli, Caprioli & Associés

Paolo De Lutiis, Telecom Italia

Jean-François Duchas, Bouygues Telecom

Christophe Delaure, Qualys Inc.

François Gratiolet, Qualys Inc.

Stéphane Lemée, Cassidian (an EADS company)

Stéphane Lu, BNP Paribas

Jean-Michel Perrin, Groupe La Poste

Axel Rennoch, Fraunhofer Fokus

# Annex B (informative): Bibliography

MITRE CybOX™ Version 1.0 (November 2012): "Cyber Observable eXpression - A Structured Language for Cyber Observables".

MITRE STIX™ Version 1.0 (Mid 2012): "Structured Threat Information eXpression".

MITRE CAPEC™ Version 2.0 (April 2013): "Common Attack Pattern Enumeration and Classification".

MITRE MAEC™ Version 4.0 (April 2013): "Malware Attribute Enumeration and Characterization".

# List of figures

# History

| Document history | | |
|---|---|---|
| V1.1.1 | December 2013 | Publication |
| | | |
| | | |
| | | |
| | | |