



Filling the gap in the Cyber Defence and Security Information and Event Management standardization

Today, reference frameworks in the cyber defence and security information and event management (SIEM) fields are often missing or are very poor, thus hindering bench-marking of IT security controls. As a result, we need IT security indicators related to event classification models.

ETSI has created an Industry Specification Group for Information Security Indicators (ISG ISI) to address this matter. ISG ISI will overcome real-world difficulties such as standards being too technical, ill-positioned or not well structured, by relying on a strong vision, while at the same time focusing on implementation. It is necessary to find a balance between security governance and technology, in order to gain support from IT and security managers and decision makers. Experience gathering being key in this matter, ETSI ISG ISI (launched during autumn 2011) is based on 7 years of hands-on experience and the frameworks of a European network of grassroots user associations in cyber defence and SIEM from France, UK, Germany, Italy, Belgium and Luxembourg.

Objectives of ISG ISI

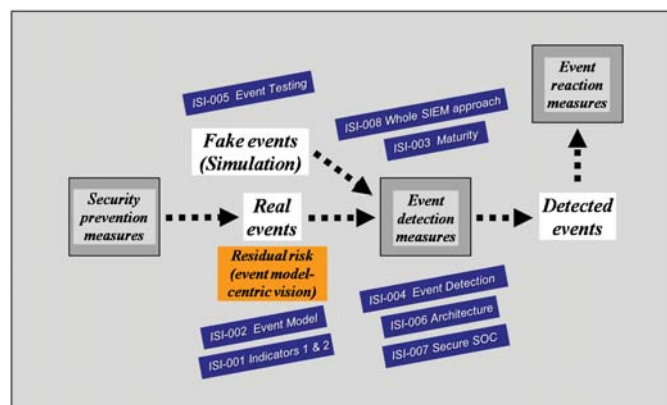
The objectives of ISG ISI are to address the full scope of the main missing security event detection issues through 8 new specifications, while being strictly compliant to ISO 2700x IT security standards:

- ISI Indicators (ISI-001-1 and its associated user guide ISI-001-2), a powerful way to assess security measures level of effectiveness through a full set of some 100 indicators,
- ISI Event Model (ISI-002), a comprehensive security event classification model covering incidents, vulnerabilities and nonconformities (with detailed taxonomy and representation),
- ISI Maturity (ISI-003), which aims at assessing the maturity level regarding overall event detection through dedicated Key Security Performance Indicators covering technology, people and processes,
- ISI Event Detection (ISI-004) demonstrates through examples how to produce indicators and how to detect the related events with various means and methods, with categories of use cases/symptoms,
- ISI Event Testing (ISI-005), proposes a way to produce security events and to test the effectiveness of existing detection means.
- ISI Measurement Architecture (ISI-006) aims at working out an ISI-compliant Measurement and Event Management Architecture for Cyber Security and Safety
- ISI Secure SOC (ISI-007) is a set of requirements to build and operate a secure SOC (Security Operations Center) addressing technical, human and process aspects
- ISI Whole SIEM approach (ISI-008) describes a whole SIEM (CERT/SOC based) approach positioning all ISI aspects and specifications

The strength of these Group Specifications (GSs) lies in the fact that they are already in use in about 100 large companies or organizations world-wide and have proven their effectiveness in several aspects:

- Providing a far more accurate knowledge of both threats and vulnerabilities through detailed state-of-the-art data regarding the main types of security events (Building up future advanced threat intelligence),
- Reconciling top-down (security governance) and bottom-up (IT ground operations) approaches, through clear event detection objectives,
- Bringing new information to decide the best trade-offs between IT security prevention and security event detection and response.

GS ISG ISI Series Summary Definition

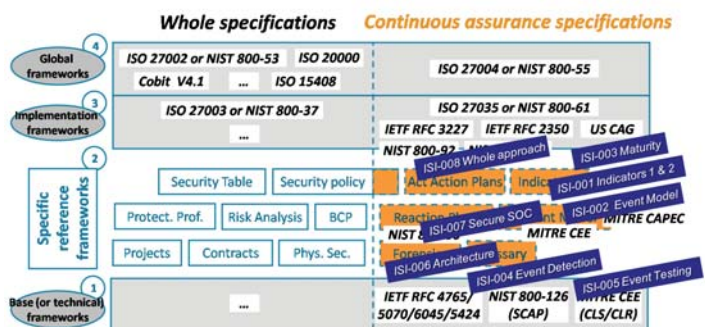


These contributions are decisive stepping stones towards a truly professional and more mature “Dynamic IT security”, beyond Risk management and Information Security Management Systems.

Role of the 8 ISI specifications

- Dedicated to security operational indicators, Group Specifications ISI-001-1 and ISI-001-2 provide a set of measurements to provide management with a reasonable level of confidence regarding the continuous assessment of an organization's security settings.
- Closely related to these two specifications, GS ISI-002 provides a full taxonomy to thoroughly describe all IT security events (and also some non-IT security events) and presents an original classification model that leverages current international best practices and allows for a range of diversified and powerful uses.
- ISI-003 GS builds a dedicated maturity scale, based on hands-on experience and relying on some of the US CAG reference framework critical controls. This is another missing piece in overall event detection. The level of maturity in this area is among the weakest in the IT security. It complements ISI-005 (which is more in-depth and more focused on a case-by-case approach).
- ISI-004 GS is the "engineering" part of the series, and presents a comprehensive classification of the main symptoms/use cases to be sought after in system traces in order to reveal stealthy incidents. The goal is also to demonstrate some powerful means and methods of detection through examples of frequent security events.
- ISI-005 GS is the key for credibility and return on investment as it dramatically improves event detection rates which are currently very low for so many types of events. Being able to rely on precise testing scenarios for a typical set of security events is therefore of utmost importance to measure the performance of systems and tools.
- GS ISI-006, which is another engineering part of the series and complements ISI-004, focuses on the design of a cybersecurity language to model threat intelligence information and enable detection tools interoperability
- GS ISI-007, in a context where SOCs are often real control towers within companies, proposes comprehensive guidelines to build a secure SOC, especially regarding the architecture aspects
- GS ISI-008 explains how to make SIEM a whole approach, which is truly integrated within an overall organization-wide and not only IT-oriented cyber defense

ISI Work Items positioned against other standards



As shown in the figure, this 8-part series complements all major existing security standards with continuous assurance at the operational level, and with clear correspondence or compatibility with most of them.

The availability and use of this 8-part series of ISI Group Specifications will have the following impact:

- Across the board frameworks for all industry sectors (which could complement the Mitre SCAP standard, which deals in particular with naming and categorizing vulnerabilities and nonconformities),
- Establishment of dependable European state-of-the-art data, with the possibility of centralized databases (further than some existing large databases, such as DataLossDB or the Identity Theft Resource Center),
- Basis for a full set of metrics to evaluate the quality and effectiveness of security equipment (bringing the two worlds of cyber defence and product certification closer).

For further details on ISI please visit: <http://portal.etsi.org/isi>

Q3 2016

ETSI produces globally-applicable standards for Information and Communications Technologies (ICT), including fixed, mobile, radio, converged, aeronautical, broadcast and internet technologies and is officially recognized by the European Union as a European Standards Organization. ETSI is an independent, not-for-profit association whose more than 800 member companies and organizations, drawn from 65 countries across five continents, determine its work programme and participate directly in its work.

For further information, please visit: www.etsi.org

ETSI, 650 Route des Lucioles, 06921 Sophia Antipolis Cedex, France. Tel: +33 (0)4 92 94 42 00 - info@etsi.org