Welcome to the World of Standards

ETSI World Class Standards

ETSI ISI-00x : A full set of new standards in Cyber Defence

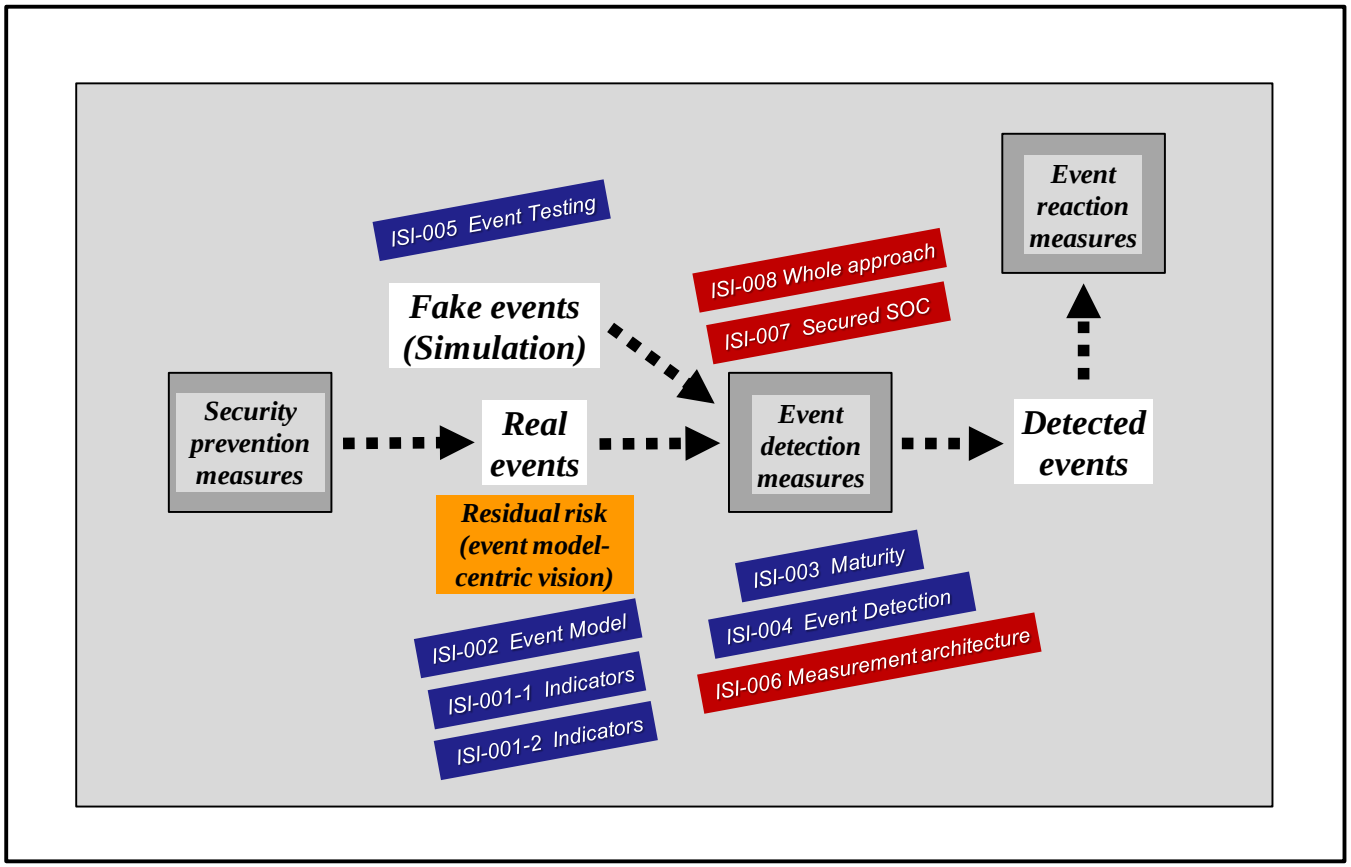
Gerard Gaudin (Chair of ETSI ISG ISI)

Reference frameworks missing and hindering IT security controls measurement

- **At first and above all, standards for IT security indicators and for related event classification models are missing (or are still very poor)**
- **Overcome past genuine difficulties**
  - Too technical or not well structured standards (although useful for some development or pen test purposes)
  - Strong vision required together with adjustment time through implementation (right aggregation level or scope of indicators)
- **Find out the *half way* between security governance understanding and ground technical positioning and skills =**
  - Gain support from IT and security managers and decision makers
- **Create an enterprise-wide common language and bring closer governance/management and technical/security experts**

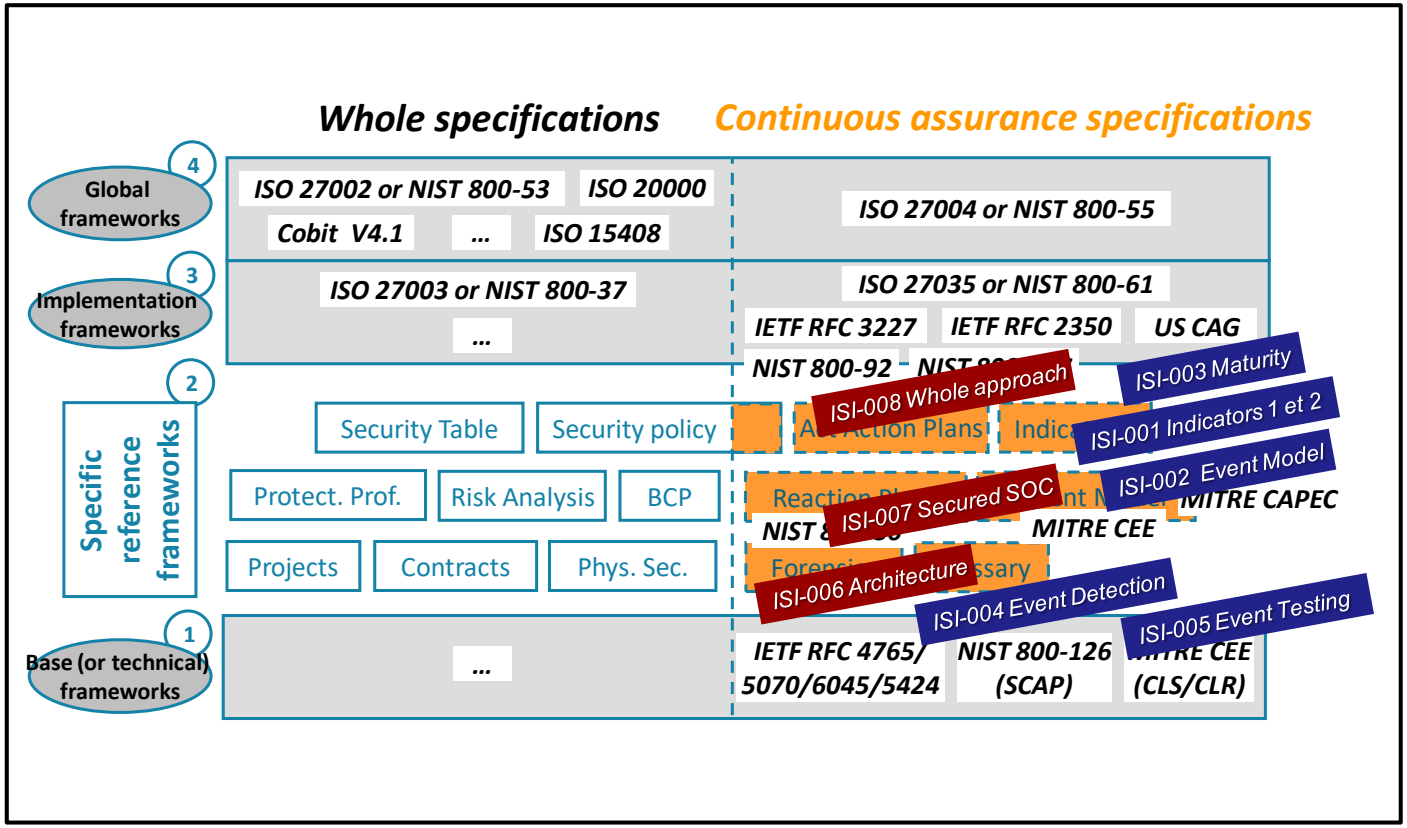
ISI Work Items definition & positioning (security incident detection field)

Addressing the full scope of security incident detection issues



A full set of standards at the crossroads of governance and technical expertise

ISI Work Items positioned against other standards



A full set of 98 indicators enabling accurate benchmarking

- **State-of-the-art statistical figures available**
  - Figures collected in 4 western countries (in US and Europe) through a panel of 15 advanced and mature companies
  - Average figures worked out with levels of scattering (Cf. trustworthiness)
  - Effective use by some European companies to benchmark their technical capabilities and their employees' behaviour improvement as regards security hygiene
  - ***An up-and-coming way ahead with ISI-006 (automatic production of indicators using Big Data), and serious hope of <u>replicability</u>***

	State-of-the-art (by month)	Country deviation	Level of scattering	Level of detection imprecision	Reference industry base	Perimeter applicable to indicator	Source (s)	Periodicity
IEX_ DOS.1	0,008 DDoS attack	No	80 % against state-of-the-art (between -50 % and +50 %)	1	Standard	By Web site	Panel of 15	Quarter
IEX_ MLW.4	1,5 malware successfully installed on servers	No	80 % against state-of-the-art (between -35 % and +65 %)	3	Standard	By set of 10,000 servers	Panel of 15	Quarter

Many diversified uses

The richness of a unique positioning at the crossroads of technical expertise and governance (developing the vision around indicators which epitomize the approach)

A. ***Speed up progress in Cybersecurity*** (through seriousness and alignment with management concerns)

Upper level
- **1.** Government Auditors
- **2.** Business executives
- **3.** General management and CISO
- **4.** Human resources and management

Lower level
- **5.** IT Operations and Production executives
- **6.** IT Engineering executives

B. ***Stimulate exchanges within the profession*** (further to those already existing in Cybersecurity communities)

Lower level
- **7.** Collect and share experience on monitoring methods/use cases for major types of incidents/vulnerabilities/nonconformities
- **8.** Make it easier to notify authorities (NIS Directive, GDPR, …) and enable Security Government agencies to provide overviews to the EU commission

1st Use implemented

Position the ETSI ISI indicators against ISO 27002 controls = provide more assurance to governance & auditors

ISO 27002 control areas	Incident type indicators	Vulnerability (behavioural, software, configuration, general security) type indicators	Comments
A5			Non-continuous checking
A6			Purely organisational issues
A7	IWH_UNA.1	VTC_NRG.1 VOR_PRT.1	Information classification + asset management
A8	IMF_LOM.1 IDB_UID.1 IDB_RGH.1 to 7 IDB_IDB.1 IDB_MIS.1 IDB_IAC.1 IDB_LOG.1	VBH_PRC.1 to 6 VBH_IAC.1 to 2 VBH_FTR.1 to 3 VBH_WTI. 1 to 6 VBH_PSW.1 to 3 VBH_RGH.1 VBH_HUW.1 to 2	Focus on deviant internal behaviours
A9	IEX_PHY.1	VTC_PHY.1	Marginal topic for a SIEM approach
...	...	...	...
A15	IMF_TRF.2 to 3	VBH_IAC.2 VBH_WTI.2 VBH_WTI.6 VBH_RGH.1 VCF_DIS.1 VCF_TRF.1 VCF_FWR.1 VCF_ARN.1 VCF_UAC.1 to 3 VTC_IDS.1	Focus on configuration vulnerabilities or non-conformities

An already wide recognition in different arenas

- In the standardization world through official liaisons with ISO JTC1 SC27 and ITU-T SG 17 Q4
- Adopted by some Information Security Government Agencies
- In the NIS Platform 3rd WG (see document “Business Cases and Innovation Paths”), considered as one of 6 key directions for the future (European agenda 2020/2025)
- Referenced by ENISA in a published document “Standards and tools for exchange & processing of actionable information”
- Support and spread by the European community of Club R2GS associations (dedicated to Cyber defence/SOC/CERT)
- Compelling demonstration of main directions/uses in a key workshop with 210 participants (moderated by Gerard Gaudin) at the 2017 International Cybersecurity Forum in Lille (France)

References

- Gerard Gaudin (see LinkedIn)
- Access to a wide set of flyers, documents and specifications (see ETSI Web site and Information Security Indicators on Wikipedia for other information)