ETSI ISG ISI initiative
Summary Presentation

14 May 2014

Frederic Martinez
Secretary of ISG ISI

Fill the gap in the Cyber Defence and SIEM standardization fields (1)

Reference frameworks missing and hindering IT security measures benchmarking

- ❑ 5-year field experience in the Cyber Defence domain with the French Club R2GS gathering 45 major companies and organizations (including French Network and Information Security Agency ANSSI)
- ❑ Network of similar « grassroots » Chapters under development in Europe (UK, Germany, Luxemburg, Italy, others to come)
- ❑ Production of reference frameworks used by most Club R2GS members (sometimes on a worldwide scale)
  - ➢ Event classification model (incidents and vulnerabilities/nonconformities)
  - ➢ Full set of operational indicators
- ❑ Feasibility of benchmarking based on ***state-of-the-art statistical figures*** tied to the set of indicators has been proven

Fill the gap in the Cyber Defence and SIEM standardization fields (2)

Scope in the world regarding standardization in this field

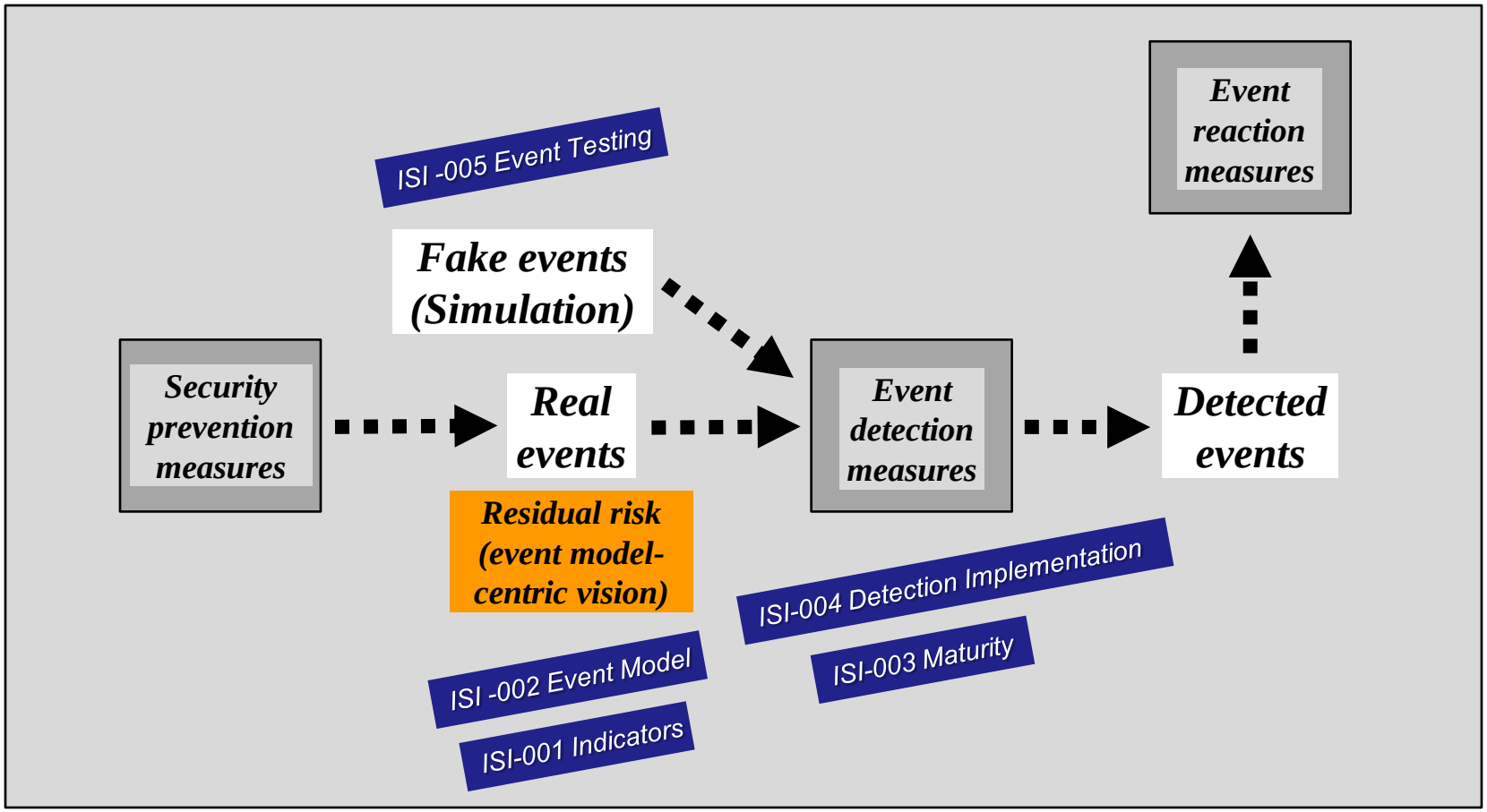
- **At first and above all, standards for IT security indicators and for tied up event classification model are missing (or are still very poor)**
- **Overcome past genuine difficulties on this matter =**
  - **Too technical or ill-positioned or not well structured standards (for example too bushy and messy MITRE CEE or CAPEC)**
  - **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**

Address the full scope of main missing security event detection issues

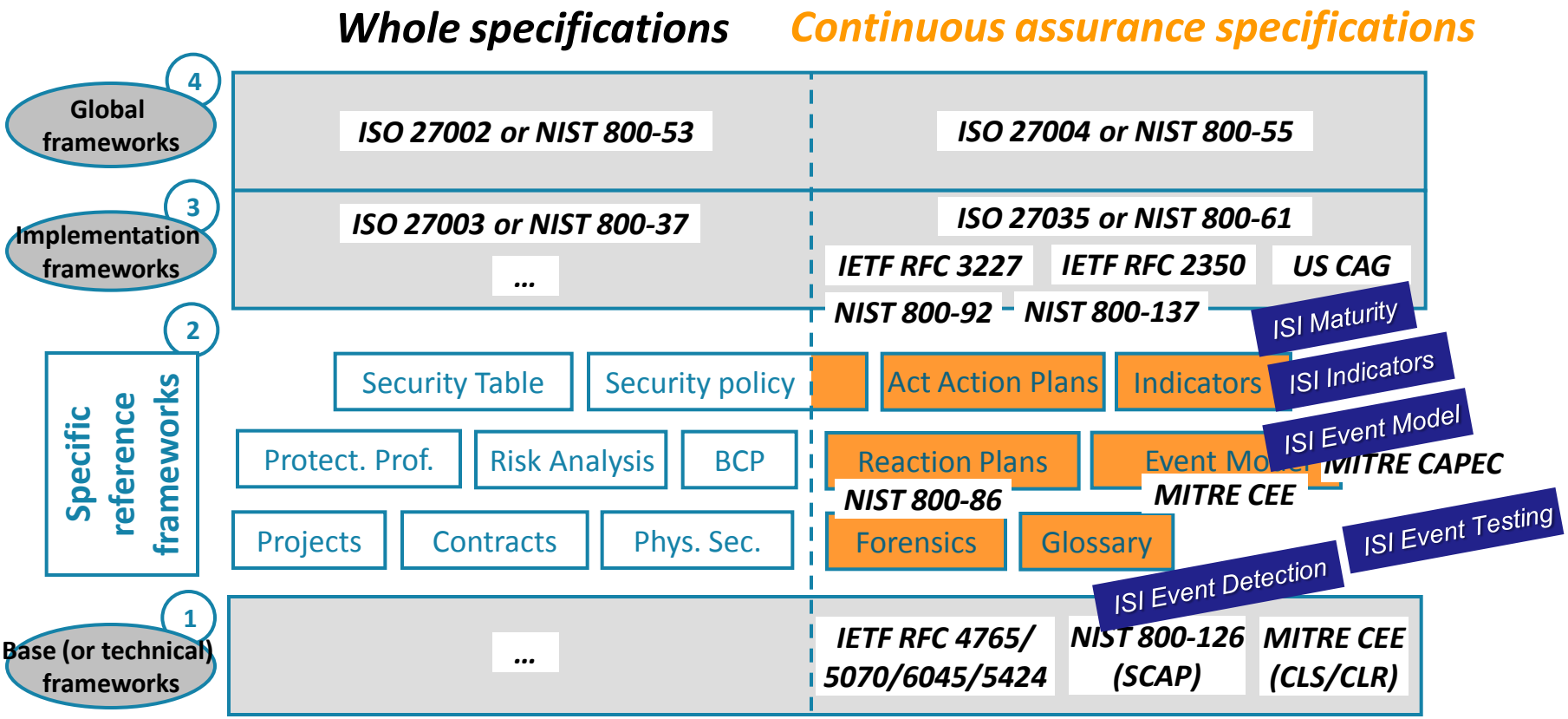
5 Work Items

- **ISI Indicators (ISI-001-1 and Guide ISI-001-2) = A powerful way to assess security measures level of application and effectiveness**
- **ISI Event Model (ISI-002) = A comprehensive security event classification model (taxonomy + representation)**
- **ISI Maturity (ISI-003) = Necessary to assess the maturity level regarding overall event detection (technology/people/process) and to weigh event detection results. Complements ISI-005 (which is more detailed and a more case by case approach)**
- **ISI Event Detection (ISI-004) = Demonstrate through examples how to produce indicators and how to detect the related events with various means and methods (with classification of hints/symptoms/artifacts)**
- **ISI Event Testing (ISI-005) = Propose a way to produce security events and to test the effectiveness of existing detection means (for major types of events)**

ISI Work Items Positioning



ISI Work Items positioned against other standards



Mrs De Soete – ISO JTC1 SC27 Vice-chair – Presentation at the 9th ETSI Security Workshop (Excerpt regarding links between ISO JTC1 SC27 and ETSI Security Cluster)

ISG ISI schedule

Most of specifications already available

- **ISG ISI started in Fall 2011 = Members of the Unit and of the 5 Work Items are European and US experts**
- **ISI Indicators (ISI-001-1 and ISI-001-2) and ISI Event Model (ISI-002) published in April 2013**
- **ISI Maturity (ISI-003) published in April 2014**
- **ISI Event Implementation (ISI-004) published in December 2013**
- **ISI Event Testing (ISI-005) started at the beginning of 2013 and might be available at the beginning of 2015**

Release of ISG ISI specifications

1st target is Europe

- Release notably through the network of associations in Europe (Club R2GS Chapters), which is structured around ISG ISI specifications
- Release through ETSI members (see 9th Security Workshop on 15/16 January 2014)
- Promotion through liaisons with ISO JTC1 SC 27 and ITU-T SG17 Q4, through national standardization bodies (AFNOR, DIN, UNI, BSI, ...), via vendors or service providers (Qualys, ...), through the IT security world community (RSA Conference, ...)
- Basis for the constitution of large data bases in Europe =
  - Independent IT security observatories providing dependable state-of-the-art figures for indicators
- This will constitute a genuine step forward for the profession (within 2 to 3 years)...