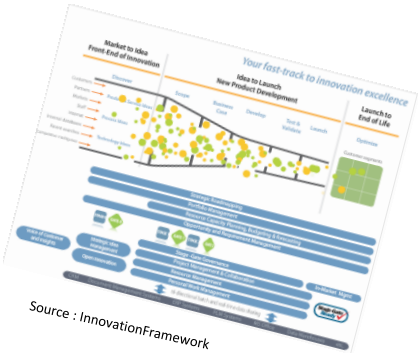
CSP Forum 2015
Cyber Security Standards

28.04.2015 - LSEC – Leaders In Security

Agenda

- About IPACSO & Innovation
- About Standards
- About Standards & Innovation
- Cyber Security Standards in
  - Business Administration : “ISO 27032 – 27001” Jan De Meer, Professor, Universities of Applied Sciences, Berlin/Brandenburg
  - Industrial Control Environments, by Wim Tindemans, CEN/CENELEC – IETF – ISA
  - Operational Security Detection “An innovative ETSI standard covering all security detection aspects (ISG ISI),”Gerard Gaudin ,G2C
  - “Vulnerability information sharing”, Ulrich Seldeslachts, LSEC
- Panel Discussion :
  - differences between standards, certifications & impact on innovation

About IPACSO



Source : InnovationFramework

"Innovation Framework for Privacy and Cyber Security Market Opportunities"

develop a structured knowledge and decision-support innovation framework for identifying, assessing and exploiting market opportunities in the privacy and cyber security technology space. …

Supporting Trustworthy ICT

Analyze the innovation process in privacy and cyber security technologies

Identify obstacles

Propose improvements, market conditions and economic incentives to invest in ICT security

Source : Sage, Innovation Process; Cranfield, Advanced Marketing Planning, InnovationCrescendo

Who?

ICT Security Innovator

ICT Security Product Development

ICT Security Market Development

ICT Security Economics Inhibitors and Incentives

Innovation Support Expertise

Cyber Security & Privacy Research

IPACSO
Innovation Methodologies State of the Art
Innovation Framework
Market & Regulatory Environment
Industry Analysis
Technology and Research
Bootcamps Framework
Innovation Bootcamps

Targetted to

Cyber Security & Privacy Innovators and Entrepreneurs

Cyber Security & Privacy Researchers

Business Brokers & PE

Policy Makers & Research Agenda

For Privacy & Cyber Security Innovators

Source : Innovationmanagement.se

- Innovation Management Support Tools
  - Provide access to State of the Art Innovation methodologies, applied to ICT Security
  - Innovation Use Cases & Best Practices
  - Innovation Framework for Cyber Security & Privacy
- Marketing Support
  - Provide access to Cyber Security & Privacy Market Assessment
  - Market and Regulatory Environment Analysis Support
  - Cyber Security & Privacy Market knowledgebase
  - Cyber Security & Privacy Technology & Research Spectrum
- Facilitating identification of Inhibitors and Incentives
  - Cyber Security & Privacy Economic Incentives
  - Access support to State of the Art Cyber Security & Privacy Research
- Training & support
  - Innovation Bootcamps and training packages
  - Access to Brokers and Corporate Development Support
- ICT Innovation Awards
  - Marketing of ICT Security Innovators – publishing cases and case studies
  - Representation towards Private Equity industry

IPACSO Innovation Framework

IPACSO Standards Overview

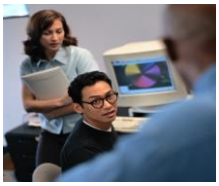
Guidance Framework/Initiative	Overview
AICI CSA Enterprise Architecture	Formerly known as the Trusted Cloud Initiative, CSA initiative that helps cloud providers develop industry-recommended, secure and interoperable identity, access and compliance management configurations, and practices.
NIST Critical Infrastructure Protection Framework	Provides a structure that organisations, regulators and customers can use to create, guide, assess or improve comprehensive cybersec programs. *http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf*
I ET NIST SP800-53	Provides a catalog of security and privacy controls for federal information systems and organisations and a process for selecting contro protect organisational operations (including mission, functions, image, and reputation), organisational assets, individuals, other organisations, and the Nation from a diverse set of threats including hostile cyber attacks, natural disasters, structural failures, and hu errors. *http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf*
C FedF PCI DSS	Requirements and standards for storage and processing of payment card data *https://www.pcisecuritystandards.org/documents/PCI_DSS_v3.pdf*
C I ISO/IEC 27001-2013	Specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organisation. It also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organisation. The requirements set out in ISO/IEC 27001:2013 are generic and are intended to be applicable to all organisations, regardless of type, size or nature. *http://www.iso.org/iso/catalogue_detail?csnumber=54534*
NERC CIP	Set of Critical Infrastructure Standards developed by North American Electric Reliability Corporation *http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx*

Standards Overview

Source : ICES 2013

Standards Overview

- What are standards anyway?
  - Technical specification which either does or is intended to provide a common design for a product
- Why are standards important?
  - Networked world; convergence
  - One means of fostering interoperability
- How are standards developed?
  - By a single company
  - By a few companies
  - By a large number of companies



Why Standards

- Standardisation is a key factor in support of a number of government policies, including competitiveness, innovation, science and technology.
- Its importance is growing with the globalisation, the convergence of technologies and a growing knowledge economy.

Source : The UK Government Public Policy Interest in Standardisation (2009),– DIUS (Department for Innovation, Universities and Skills)

Incentive to interconnect

- Value of network depends on size, so there are strong social benefits to interoperability
- But not necessarily private benefits due to loss of monopoly power
  - Bell System in 1890s and long distance
  - Marconi Intl Marine Corp
- But even dominant incumbent may find interconnection compelling
  - Your value = your share x industry value
  - If industry value increases dramatically, may be worth loss of monopoly
  - See auto industry, next slide

Source : Hal K. Varian, 2012

Historical standards

- Standardization as cost saver
- Auto parts standardization c. 1910
  - Risk avoidance for suppliers
  - Economies of scale for manufacturers
  - Lack of interest on part of Ford/GM
  - Role of Society of Automotive Engineers
  - Eventual adoption of standards

Source : Hal K. Varian, 2012

Standard Wars

- competing standards :
  - VCRs (Sony/Betamax v VHS)
  - HD DVD v BluRay
  - Original CD and DVD standards
  - Dominant players set standard :
    - Adobe PDF
    - Microsoft SMB and Samba
  - AM stereo
    - Auto industry invested, radio didn't
  - Digital wireless phones (1998)
    - Europe: GSM
    - US: GSM, TDMA (cousin of GSM), CDMA
      - TDMA: 5 million
      - CDMA: 2.5 million
      - GSM: 1 million

- Strategies in standards wars
  - Penetration pricing
    - AdWords
  - Alliances with Complementors
    - DVD and Hollywood
  - Expectations management
    - Dangers: Osborne computer
  - Commitment to low prices
    - Internet Explorer

Source : Hal K. Varian, 2012

Standards setting competition

- Standards war: competing standards
  - HD DVD v BluRay
- Negotiation: want a common standard, negotiate to determine it
  - Original CD and DVD standards
- Standards leader: dominant firm creates standard, followers adapt to it
  - Adobe PDF
  - Microsoft SMB [http://ubiqx.org/cifs/SMB.html]

Defining Types of Standards

- Open vs Industry
  - "Open" standards – technical specifications that have been approved or ratified through an open consensus based process, publicly available, vendor neutral, licensed under RAND terms (with or without a royalty or fee)
  - Proprietary or Industry standards – technical specifications maintained by a private entity or group of cooperating entities, and licensed under commercial terms
- De Juro vs De Facto
  - De Juro : standards according to law, are endorsed by a formal standards organization. The organization ratifies each standard through its official procedures and gives the standard its stamp of approval.
  - De-Facto : standards in actuality, are adopted widely by an industry and its customers. They are also known as market-driven standards.

Source : Microsoft, LSEC, electronicdesign.com

Definitions of "Openness"

- "Open" is not a legal term
- "Open" as an adjective
  - Can take on many meanings
  - Can lead to use as a verb, with adverse impact on IP and innovation
- Traditional definition of "open standard"
  - Standards developed or ratified through an open, consensus process
  - Admission open to all
  - Covered by an open and transparent IPR policy
  - Contributors license essential IPRs to implementers on Reasonable and Non-Discriminatory (RAND) terms (with or without royalties/fees)

"Open Standard"

- Traditional definition reaffirmed by:
  - **Global Standards Collaboration (GSC)** - http://www.itu.int/ITU-T/gsc/gsc10/index.html - **Resolution GSC-10/04: (Joint Session) Open Standards**
  - **ITU-T** - **http://www.itu.int/ITU-T/othergroups/ipr-adhoc/openstandards.html**
  - **American National Standards Institute (ANSI)** - **http://publicaa.ansi.org/sites/apdl/Documents/Standards%20Activities/Critical%20Issues%20Papers/Griffin%20-%20Open%20Standards%20-%2005-05.doc**

More Recent Definitions…

- New uses of the term and confusion
- "Free to implement"
  - Very few standards bodies mandate a RANDZ approach
  - All essential patent claims may not be covered by such a policy
- "Free to use freely"
  - Is there any standards body that mandates such an approach?

Implications of new definitions

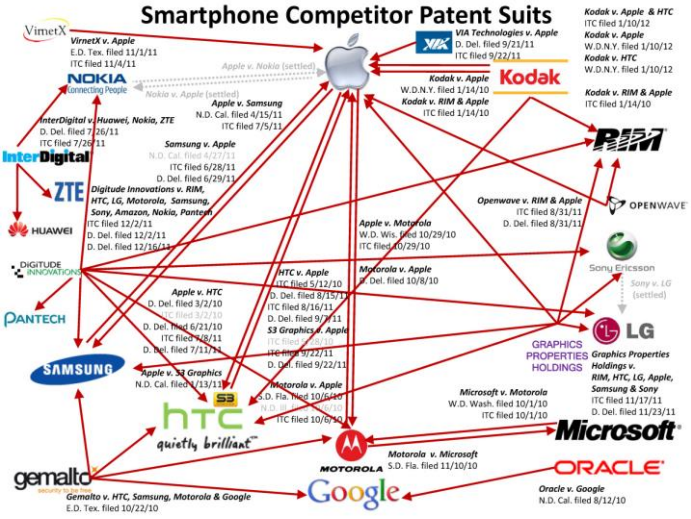
- If “open” means royalty free…
  - SSO desire to attract key technology holders
  - Will they come?
  - And the rest of the standards world?
- The latest twist… disclosure obligations
  - How much and when should a participant or contributor disclose about the existence of patents?
  - Requirements for searches?
  - About specific license terms?

Value of standards

- “Standards are a proven tool for economic development” (ITU)
- “Standards are not *designed with a specific economic outcome in mind, but to increase safety or manage risk. To the* extent that accidents or risks lead to economic costs then their prevention through the use of Standards“ (Centre for International Economics, 2006)
- “Standards and patents both aim to promote innovation and boost the economy.” (ITU)
- “a prime means of diffusing innovation through the whole economy, ensuring that the bulk of firms do not lag too far behind the early adopters of new ideas” (Global ICT Standards organization in India)
- From the perspective of the user, developer or implementer (micro):
  - Lower prices, more suppliers, less lock-in, more complementary goods
- From the societal / economic perspective (macro):
  - (+) Standards encourage technical change, innovation and competition, facilitate international trade.
  - (-) Standards can convey special power to owner, may obstruct market access, and can hamper competition and innovation

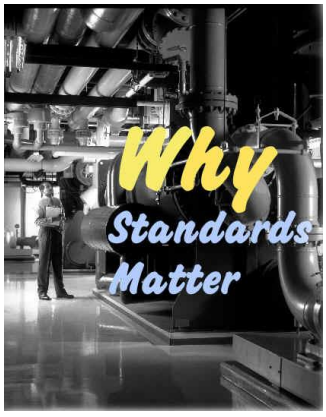
Source : GISFI, ITU,

Value of standards



Source : Smartphone Patent Wards Explained, 2012

So (why) do we need standards in Cyber Security & Privacy?



CSP/ISO –MCE150428

Jan de Meer, ssl.eu GmbH

28.4.2015

ISO SC27 WG4 IS 27032 –
Cyber Security Guidelines

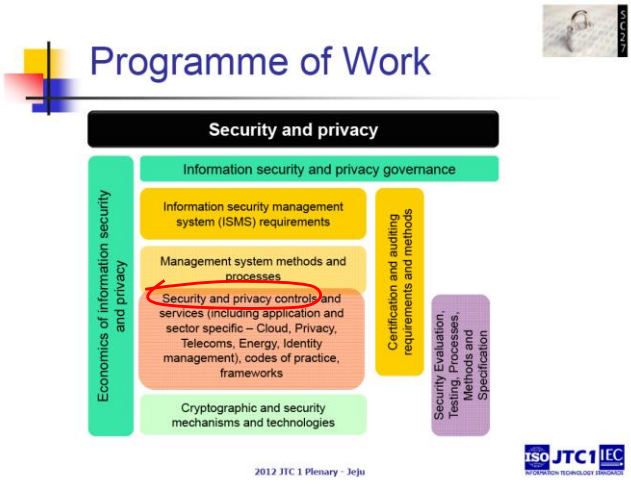
ISO SC27 WG4 IS27032 – Walter Fumy SC27 Chair (2012 JTC1 Plenary)

Standing Document 4 (SD4)
ISO/IEC JTC1/SC 27 Programme of Work

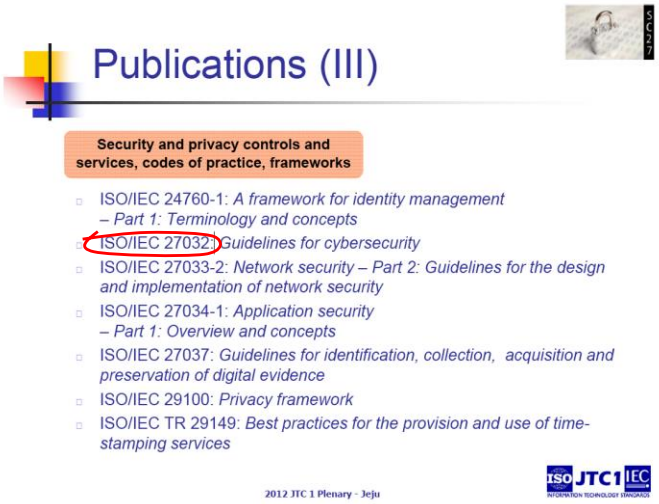
ISO/IEC JTC 1/SC 27 N14254

Project number	Status 2015-03	ISO/IEC Number		WG Editor / Rapporteur	NP Doc. / WD Recomm/ Justifica-tion	CD / PDAM /PDTR /PDTS	DIS / DAM	IS / AMD / TR / TS
1.27.62	IS	27032:2012-07-15 (1st edition)	Guidelines for cybersecurity	4	1st JTC 1 systematic review in 2017			1st pre-review in 2015

ISO SC27 WG4 IS27032 – Walter Fumy SC27 Chair (2012 JTC1 Plenary)



ISO SC27 WG4 IS27032 –
Walter Fumy SC27 Chair (2012 JTC1 Plenary)



ISO SC27 WG4 IS27032 –
N0061 SWG5 N0135 Collection of Standards related to IoT

Template for collection of Data related to the Internet of Things

This template is used to collect data for an all-encompassing spreadsheet on standards related to the Internet of Things. The goal is to include all standards from all Standards Development Organizations that can possibly relate to the IoT. The top of the spreadsheet is locked and contains the column titles, some possible entries for several of the columns and some examples of data entered into the spreadsheet. You are NOT restricted to the suggested entries. If you feel that there is an ambiguity in your entry please feel free to provide extra information.

Title of Deliverable	Scope of deliverable	SDO	Current Status	Target Date	Type of Deliverable	Technology Domain	Specific Technology	Application Domain	Issues	
Possible Entries for this column	*From the document*	*Possible Entries for this column*	*Possible Entries for this column*		*Possible Entries for this column*	*Possible Entries for this column*	*Possible Entries for this column*	*Possible Entries for this column*		
Standard		ANSI	Published		Technology	Localization and Tracking	RFID	Water monitoring		
Technical report		ISO	CD		Conformance Testing	Communications and Networking	QR Code	Power grid conditioning		
Recommendation		IEC	Recommendation		Interoperability Testing	Applications	6LoWPAN	Retail goods tracking		
RFC		AIM			Performance	Processing/Computing	CDMA	Building facilities monitoring		
		ITU-T				Security, Privacy, and Authentication	GSM	Accessibility		
						Data Structure/Formats				
						Data Carrier				
						etc.	etc.	etc.		

ISO/IEC 27032 Guidelines for cybersecurity	This International Standard provides guidance for improving the state of Cybersecurity, drawing out the unique aspects of that activity and its dependencies on other security domains, in particular: information security, network security, internet security, and critical information infrastructure protection (CIIP). It covers the baseline security practices for stakeholders in the Cyberspace.	ISO/IEC JTC 1/SC 27	Published 1st ed.		IS

ISO SC27 WG4 IS 27032 –
(some Notions from SC27 N8624 2010-06-15)

- Cybercrime:= where Cyberspace is source, tool, target, place for illegal activities;
- Cybersafety:= condition of being protected
  - against physical, social, spiritual, financial, political, emotional, occupational, psychological, educational or
  - other types or consequences of failure, damage, error, accident, harm
  - or any other event in the Cyberspace which could be considered non-desirable;
- Cybersecurity:= preservation of Confidentiality, Integrity, Availability of Information in the Cyberspace;
- Cyberspace:= complex environment resulting from interaction of people, SW, services of the internet by means of technological devices and networks which does not exist in any physical form(?);

Agenda

- Welcome
- Overview ISA & ISA Belgie
- Why using standards & ISA
- Introduction to the standard
- Awareness
- Models
- Q&A

Who is ISA ?

- International Society of Automation
- Headquarter in North Carolina, USA
- European Headquarter in Eindhoven, The Netherlands
- > 30.000 members worldwide
- Activities:
  - Develop standards
  - Certify industry professionals
  - Provide training
  - Publish books
  - Organize conferences

ISA-Belgium Section

- Part of EMEA organization ISA (known as District 12)
- Section was not active since 1999 and is reactivated in 2011
- www.isa-belgium.org
- Adress:

  Kasteelhoekstraat 1
  1820 Perk
  02-253 01 55

- Board:

Kris Adriaenssens	kris.adriaenssens@isa-belgium.org
Wim Tindemans	wim.tindemans@isa-belgium.org
Marc Blekkink	marc.blekkink@isa-belgium.org

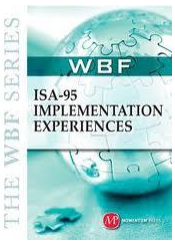
Standards

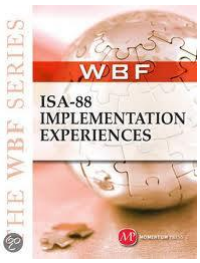
- ISA-84
  - addresses the application of safety instrumented systems for the Process Industries
- ISA-88
  - the international standard to help industries to produce in a flexible way
- ISA-95
  - the international standard for the integration of enterprise and control systems
- ISA-99
  - current assessment of security tools and technologies that apply to the Manufacturing and Control Systems environment
- ISA-100
  - Wireless Systems for Industrial Automation

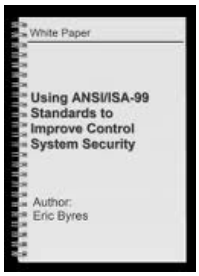
Why using standards & ISA?

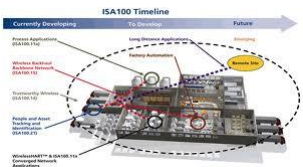
- Top players in automation software market adopts the standard in their solutions
- Uniform language between end user, integrator and supplier
- Faster implementation of solutions
- Unified communication methodologies

Practical examples









Position of ISA in Belgium

- IEC 61131

Membership

- Membership:
  - 110 US$/year
  - Access to standards
- Student membership:
  - 10 US$/year

- Access to all standards -> source of
- Events -> Indumation -> Networking
- Competitive advantage -> Knowledge

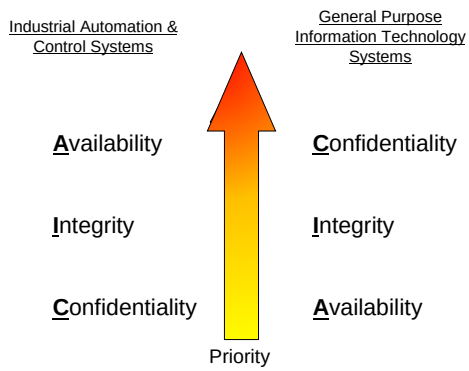
info@isa-belgium.org
www.isa-belgium.org

Introduction to

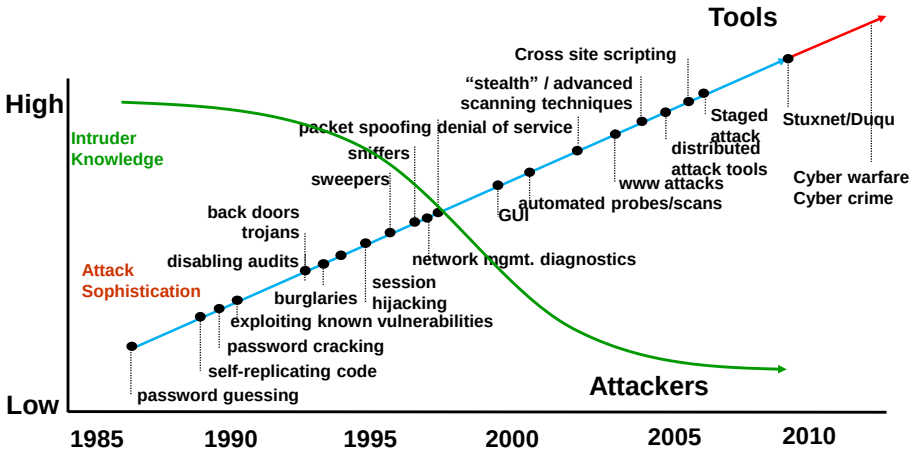
ISA/IEC-62443 (Formerly ISA-99)

Process Control Security – What's the difference?

- **Process and Office Automation: different focus**



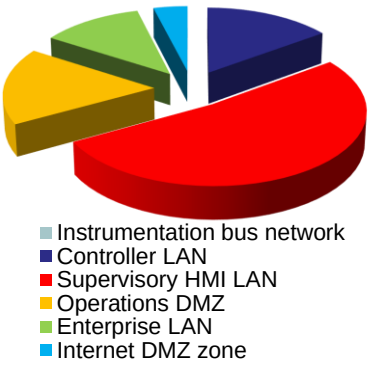
Stuxnet, a new era



Indentified in efforts

- 15 ICS assessments
- 900 hours effort
- 245 vulnerabilities

Vulnerabilities



* Source: US Department of Homeland Security

Process control systems?

- IT and automation networks are no longer separated
- Automation networks are more and more based on standard technologies
- Industry is an interesting and sensitive target
- Larger amount of viruses and Trojans
- Hacking is simple

Your process environment

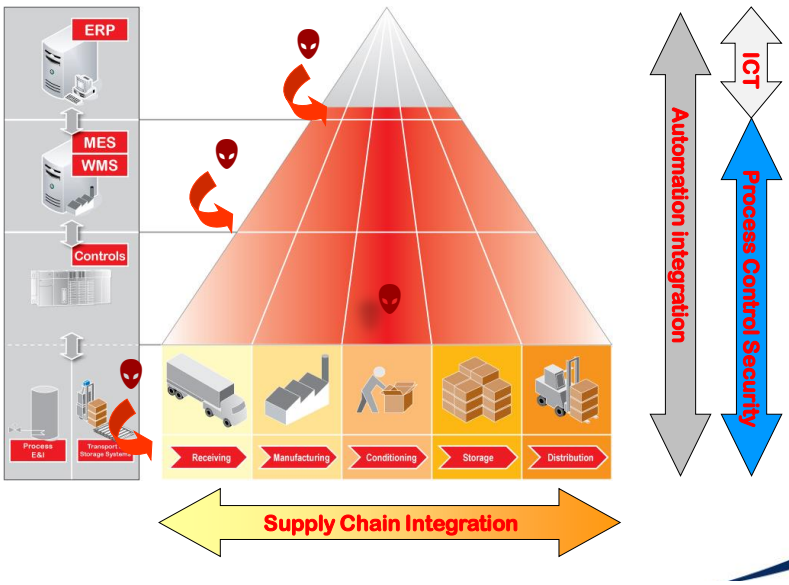
- **Changing environment**
  - Increased level of automation
  - Standardization
    - Windows
    - Networks
    - Etc.
  - Requirements of data exchange and connectivity

⇒ **Higher risk**

Every process environment a possible target

⇒**New standards, regulations and best practices have to be incorporated**

Your process environment



Possible Process Control Security incidents

- **Hack into your Process Control System**
  - Disruption / blockade installation
  - Manipulation of production data
  - Industrial espionage
  - Theft of business critical information
    - E.g. recipes…

Impact Process Control Security incidents

- **Physical damage to people, installations and environment**
- **Blockade / falling-out installations**
- **Loss of production data**
- **Damage to product quality**
- **Loss of product**

Impact Process Control Security incidents

- **Depends on different factors**
  - System criticality
  - Automation dependency
  - Presence of backup plans
- **Several impact categories**
  - Customer trust
  - Image damage
  - Legal
  - HS&E
  - Financial

What to do?

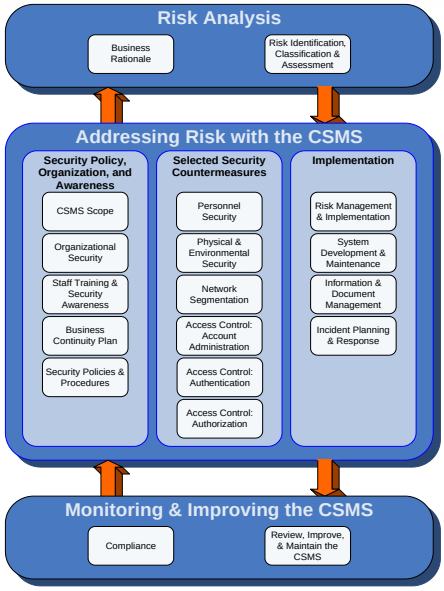
- **Reality check**
  - Increase Process Control Security awareness
  - Security starts with Awareness!
    - ✓ Top management -> shop floor people -> contractors -> visitors

- **100 % system security does not exist**
  - But: most systems can be made far more secure

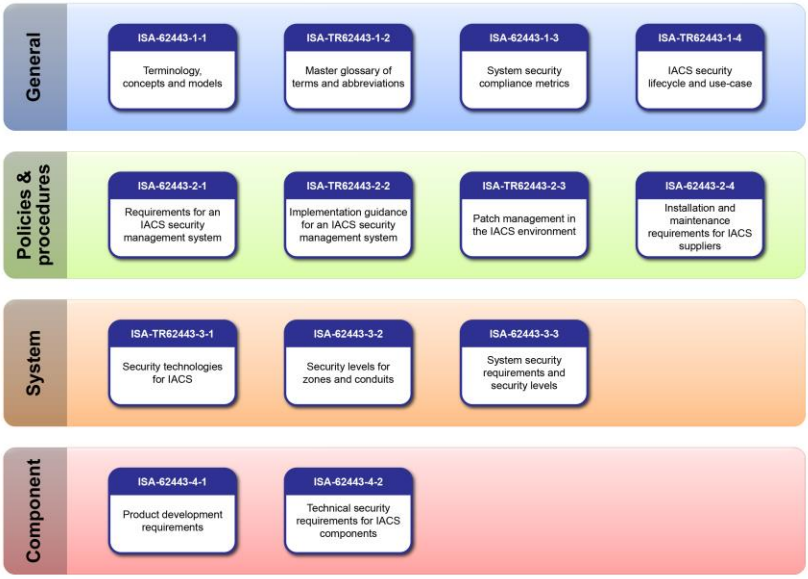
» **Implement a solid security strategy**

- Measuring and identifying risks
- Taking countermeasures and managing/mitigating risks
- Implement Defense in Depth Strategies

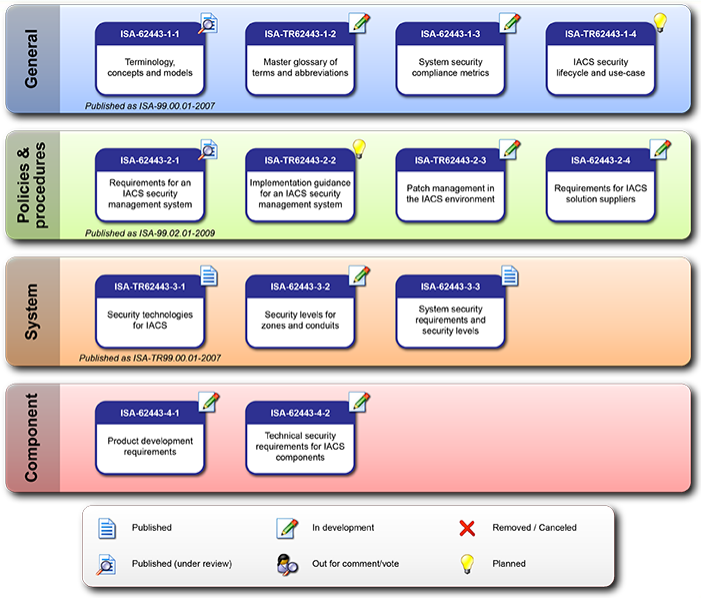
ISA99: Industrial Automation & Control Systems Security Program



ISA-62443



ISA-62443 current status



Thank you.

For more information please contact us at:

ISA Belgium VZW
Kasteelhoekstraat 1
1820 PERK
Tel. 02-253 01 55
Fax 02-252 01 55

isa-belgium.org

ISA Belgium Section

ISG ISI (Information Security Indicators)

ETSI ISG ISI initiative Summary Presentation (CSP Forum)

28 April 2015

Gerard Gaudin
Chairman of ISG ISI

ISG ISI (Information Security Indicators)

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

Reference frameworks missing and hindering IT security measures benchmarking

- **7-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 across Europe (UK, Germany, Italy, Luxembourg, Belgium)**
- **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**

ISG ISI (Information Security Indicators)

Fill the gaps 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 related event classification model are missing (or are still very poor)**
- **Overcome past genuine difficulties on this matter =**
  - **Too technical or not well structured standards (for example MITRE CEE)**
  - **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**

ISG ISI (Information Security Indicators)

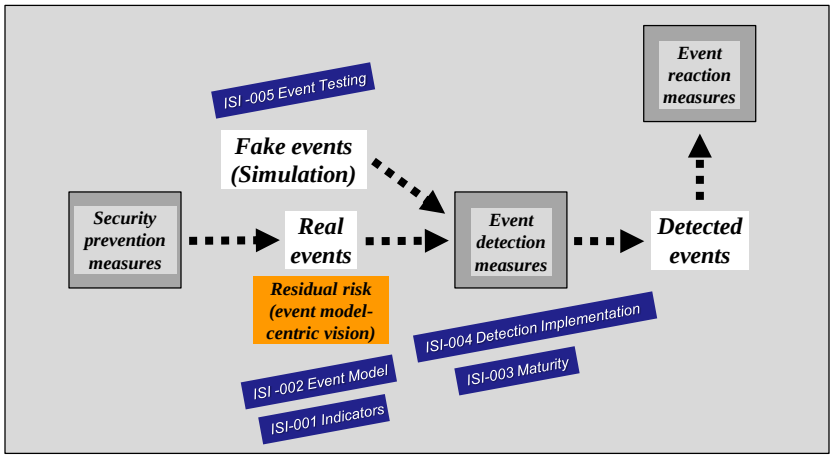
Address the full scope of main missing security event detection issues

5 Work Items closely linked together

- **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 Detection Implementation (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 capabilities (for major types of events)**

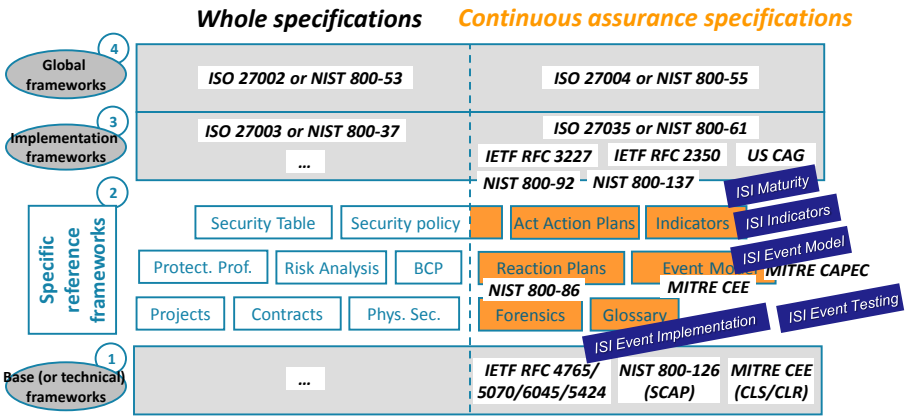
ISG ISI (Information Security Indicators)

ISI Work Items Positioning



ISG ISI (Information Security Indicators)

ISI Work Items positioned against other standards



ISG ISI (Information Security Indicators)

Why ETSI GS ISI-001 indicators are more and more used successfully

A complex mix of Key Success Factors

- ❑ Simple and easy to explain (« Elevator test » and 2-page sheet)
- ❑ However elaborate and solid methodology
- ❑ Standardized approach (ETSI) & ISO JTC1 SC27 amplifier
- ❑ Answer to increased requirements for hard data in the fuzzy cyber world
- ❑ A European Cybersecurity community under steady development supporting and spreading the approach (Club R2GS)
- ❑ A user-based approach having been continuously improved for more than 6 years
- ❑ Last but not the least … many different, practical and compelling uses ***Why?*** ***How?***

ISG ISI (Information Security Indicators)

The richness of uses at the crossroads of technical expertise and governance

- ❑ **Speed up progress in Cybersecurity** through seriousness and alignment with management concerns
  - ➢ Government Auditors – Enhanced level of assurance
  - ➢ Business executives – Better awareness of major IT risks and stakes
  - ➢ IT Operations and Production executives – Streamline OSM operations by maximizing the value of detection tools and teams
  - ➢ IT Engineering executives – RFP for SIEM or VDS tools
  - ➢ General management and CISO – Measure accurately improvement of user healthy computer behaviours in a threatening IT context
  - ➢ Human resources and management – Measure company loyalty
- ❑ **Stimulate exchanges within the profession** (further to the ones found in existing Cybersecurity communities)
  - ➢ Collect and share experience on monitoring methods/use cases for major types of incidents/vulnerabilities/nonconformities
  - ➢ Make it easier to notify authorities

ISG ISI (Information Security Indicators)

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 (Information Security Indicators)

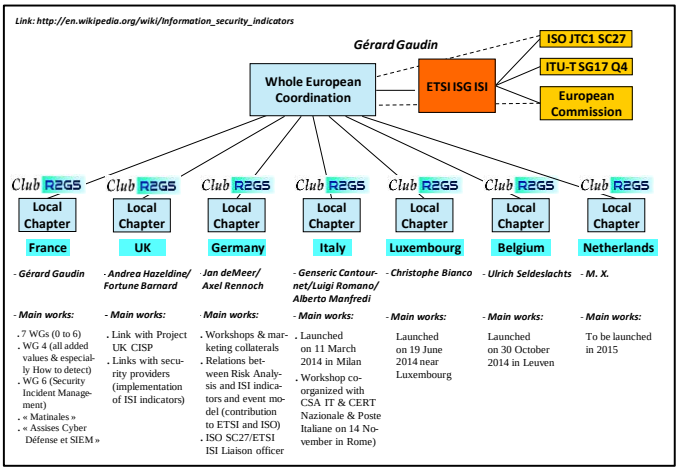
ISG ISI schedule

Most 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 Classification Model (ISI-002) published in April 2013 (Revision 1 to be published mid-2015)**
- **ISI Maturity (ISI-003) published in May 2014**
- **ISI Event Implementation (ISI-004) published in December 2013**
- **ISI Event Testing (ISI-005) to be published mid-2015**

ISG ISI (Information Security Indicators)

Standards supported across Europe, especially by the European community of Club R2GS Chapters



ETSI's Role in CYBER SECURITY

Scott CADZOW

European roots, Global outreach

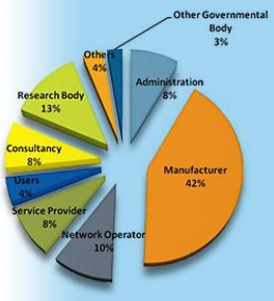
- ETSI is a world-leading standards developing organization for Information and Communication Technologies (ICT)
- Founded initially to serve European needs, ETSI has become highly-respected as a producer of technical standards for worldwide use

71

Membership

- Over **750 companies**, big and small, from **62 countries** on **5 continents**
- Manufacturers, network operators, service and content providers, national administrations, ministries, universities, research bodies, consultancies, user organizations

A powerful and dynamic mix of **skills, resources and ambitions**



72

Collaboration

- Strategic collaboration with numerous global and regional standards-making organizations and industry groupings
- Formally recognized as a European Standards Organization, with a global perspective
- Contributing technical standards to support regulation
- Defining radio frequency requirements for the technologies we standardize

73

ETSI Clusters

http://www.etsi.org/technologies-clusters/clusters

74

Areas of security standardization

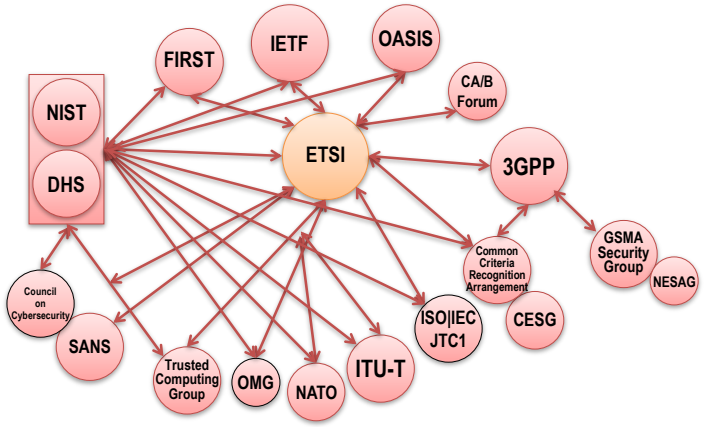
- Cyber Security
- Mobile/Wireless Comms (GSM/UMTS, TETRA, DECT…)
- Lawful Interception and Data Retention
- Electronic Signatures
- Smart Cards
- Machine-to-Machine (M2M)
- Methods for Testing and Specification (MTS)
- Emergency Communications / Public Safety
- RFID
- Intelligent Transport Systems
- Information Security Indicators
- Quantum Key Distribution (QKD)
- Identity and access management for Networks and Services (INS)
- Algorithms
- In 3GPP

75

ETSI TC CYBER

- Cyber Security Standardization
- Security of infrastructures, devices, services and protocols
- Security advice, guidance and operational security requirements to users, manufacturers and network and infrastructure operators
- Security tools and techniques to ensure security
- Creation of security specifications and alignment with work done in other TCs and ISGs
- Coordinate work with external groups such as the CSCG with CEN, CENELEC, the NIS Platform and ENISA
- Collaborate with other SDOs (ISO, ITU, NIST, ANSI...)
- Answer to policy requests on Cyber Security and ICT security in broad sense

Cyber Security SDO ecosystem



The ETSI TR 103 306 “Global Cyber Security Ecosystem “ regularly updated in order to follow the constantly evolving global Cyber Security scenario

International Collaboration in ETSI

- TC CYBER to create/keep relations with other ETSI TCs/ISGs
- CYBER as leading ETSI security body
- Reference for any other TC and technology
- Reference for Liaisons with other Standard Developing Organisations (SDOs)

TC: Technical Committee

ISG: Industry Specification Group

78

TC CYBER work items in development

- 9 open documents
  - 8 Technical Reports
  - 1 ETSI Guide

- TR 103 303, Protection measures for ICT in the context of Critical Infrastructure
- TR 103 304, PII Protection and Retention
- TR 103 305, Security Assurance by Default; Critical Security Controls for Effective Cyber Defence
- TR 103 306, Global Cyber Security Ecosystem
- TR 103 307, Security Aspects for LI and RD interfaces
- TR 103 308, A security baseline regarding LI for NFV and related platforms
- TR 103 309, Secure by Default adoption – platform security technology
- TR 103 331, Structured threat information sharing
- EG 203 310, Post Quantum Computing Impact on ICT Systems

Security Week in June 2015

	Mon 22	Tue 23	Wed 24	Thu 25	Fri 26
AM		Workshop	Workshop	**CYBER#4** **ISI#23** eIDAS	**CYBER#4**
PM	Workshop	Workshop	**Streams:** M2M/IoT ITS eIDAS HF/USER/e Health	**CYBER#4** **ISI#23** eIDAS	**CYBER#4**

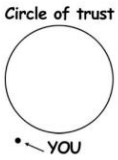
- M2M/IoT: Machine-to-Machine / Internet of Things
- ITS: Intelligent Transport Systems
- eIDAS: Electronic identification and trust services
- HF: Human Factors
- USER: User Group
- eHealth: Health ICT

80

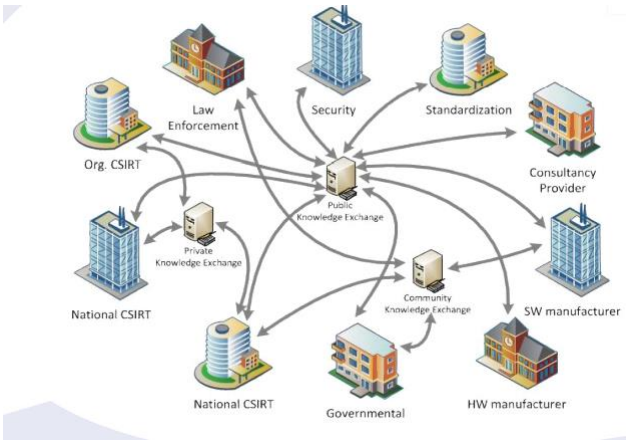
Forrester defines threat intelligence as:

Source : Forrester Research, 2014

- Details of the motivations, intent, and capabilities of internal and external threat actors. Threat intelligence includes specifics on the tactics, techniques, and procedures of these adversaries. *Threat intelligence's primary purpose is to inform business decisions regarding the risks and implications associated with threats.*
- We share at about the same speed that George R.R. Martin writes novels, which is slow
- Quid pro quo and relationship driven
- You cannot automate trust

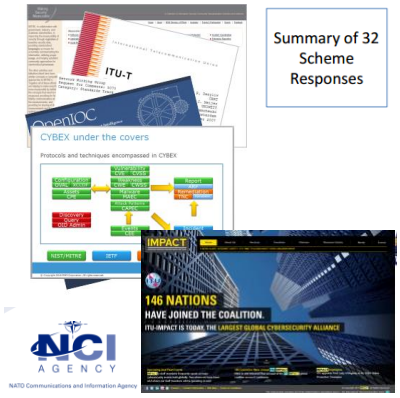


Entities Involved



Sources : NATO NIAS, 2015

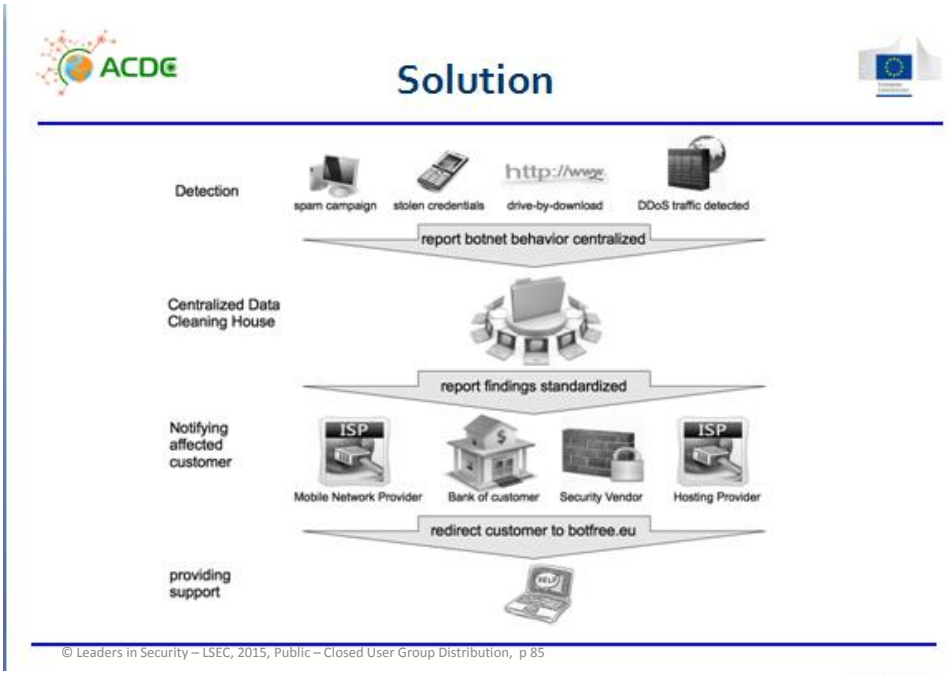
Activities in Information Sharing



Summary of 32 Scheme Responses

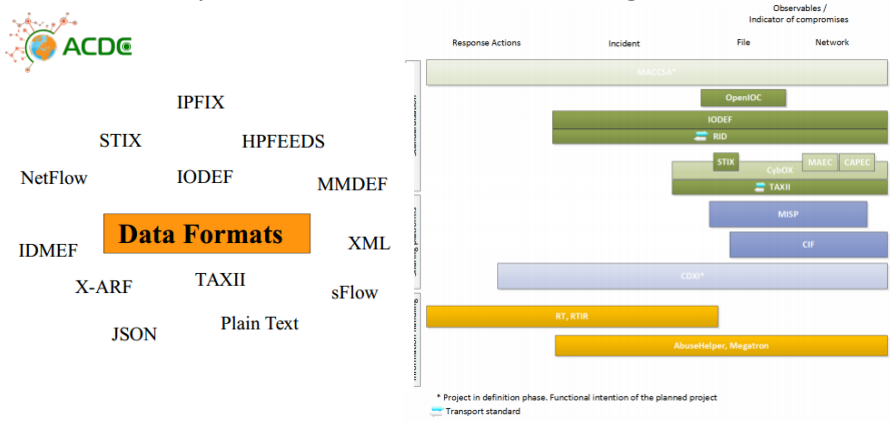
	Distribution 1	Distribution 2	Distribution 3
1	National (71%)	Regional Multinational (25%)	International (1 scheme)
2	Single Sector (75%)	Cross Sector (25%)	
3	Mandatory Participation (7%)	Discretionary Participation (93%)	
4	Free to Access Scheme (86%)	Subscription Required to Access Scheme (14%)	Both (Of the subscribing services some subset of services are free based on specific criteria) 3 Schemes
5	Information Sharing Schemes (27)	Pure Incident Notification Schemes (1)	Providing for both Incident Notification and Information Sharing (17)
6	Formal Sharing Protocol incorporated (64%)	Informal Sharing / Notification Protocol incorporated (43%)	
7	<20 Participating Organisations (43%)	>20 <40 Participating Organisations (18%)	>40 Participating Organisations (29%)
8	Email Communications Supported (57%)	Portal Sharing Platform (25%)	Support for Automated Exchange of Information & Indicators (25%)
9	Scheme Operating >1 <3 years (4)	Scheme Operating >3 years < 5 years (3)	Scheme Operating > 5 years (7)
10	Scheme has No Physical Community Meetings	Scheme has Community Meetings between 1-2 time per year (1)	Scheme has Community Meetings more than 2 time per year (11)
11	Website in place for Scheme (68%)	No Website in place	

Sources : NISP WG2 Survey, 2014; NATO NIAS, 2015, LSEC



Standards in Information Sharing

- An attempt to an overview Data Exchange Formats



Sources : ACDC, Data Format analysis, 2013, ENISA, Detect-SHARE-Protect, October 2013 – Mapping of Standardisation and Solutions for Response, Incident and IoC Information Sharing

Information Sharing

Key Learning experiences :

- Sharing is NOT
  - You give me all your information
  - I will not contribute to any of the information
  - I will secretly give this information to people
  - another secret group to learn to share
- Sharing IS
  - "Let's work together to bridge the existing silos"
  - "Collaboration and creating governance structures to limit
- legal obligations vs legal restrictions

Use Cases :

- Submission of data
- Transport of malware samples
- Transport of bulk data
- Incident reports targeted to CSIRTs
- Incident reports targeted to end users

Properties – Requirements :

- Machine and human readable
- Binary vs textual representation (e.g. XML)
- Versatility vs specialisation
- Formal specification (structure and data types)

Source : IID - 2014, ACDC - LSEC 2013 - 2014

Need for holistic threat intelligence

- Effective understanding, decision-making and action require a holistic picture of both ourselves and the adversary.
  - What are our assets? What are our missions and activities? What is our attack surface? Where are we vulnerable?
  - Who is the adversary? Where are they acting? How are they acting? What does it look like when they act? What are they targeting? What actions should we take to mitigate their actions?
- Holistic threat intelligence is not a single player sport
  - It depends on access to a wide range of information and no single entity, no matter how large, has the full picture to be consistently predictive or effective in prevention.
  - It requires sharing of information between interested parties
  - How can my detection today aid your prevention tomorrow?

Source : LSEC STIX Training, MITRE, US DHS

Need for automation

- Massive amounts of information, diverse sharing partners, rapid tempo of attack and need to respond at machine speed require automation
- Human interpretation and decision will always be involved but we need to assist them in this by letting machines do what machines do well.

Source : LSEC STIX Training, MITRE, US DHS

Standards in Information Sharing

- STIX : an industry standard under development

GitHub

OASIS
Advancing open standards for the information society

Homeland Security

MITRE

Source : ENISA, DHS, LSEC Analysis 2015

Howto : Incident Management Tools

STIX™

Effective Cyber Threat Intelligence and Information Sharing

 http://stix.mitre.org/

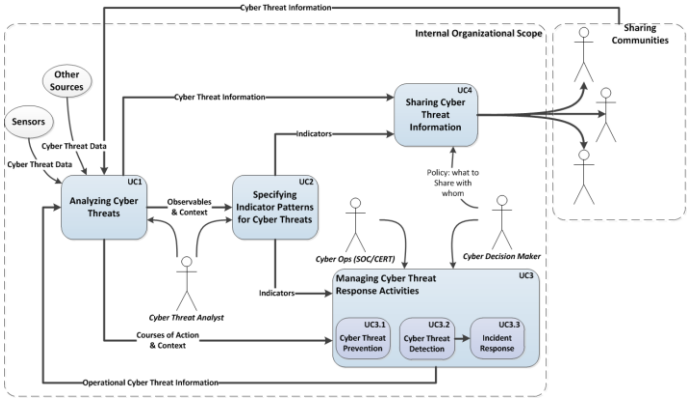
Information Sharing : commonalities, no conflict

Consider these questions:

- What activity are we seeing? — Observable
- What threats should I look for on my networks and systems and why? — Indicator
- Where has this threat been seen? — Incident
- What does it do? — TTP
- What weaknesses does this threat exploit? — ExploitTarget
- Why does it do this? — Campaign
- Who is responsible for this threat? — ThreatActor
- What can I do about it? — Course of Action

 http://stix.mitre.org/

STIX Use Case

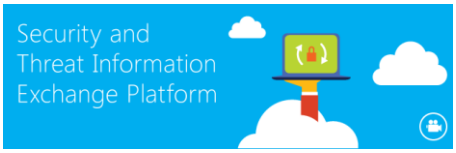


STIX provides a common mechanism for addressing structured cyber threat information across and among this full range of use cases improving consistency, efficiency, interoperability, and overall situational awareness.

Driver for innovation

- STIX has become a driver for innovation with traditional and startup companies

Microsoft Interflow: a new Security and Threat Information Exchange Platform



Lockheed Martin Integrates Cyber Security Standards into Open Source Platform

intel Security

CISCO

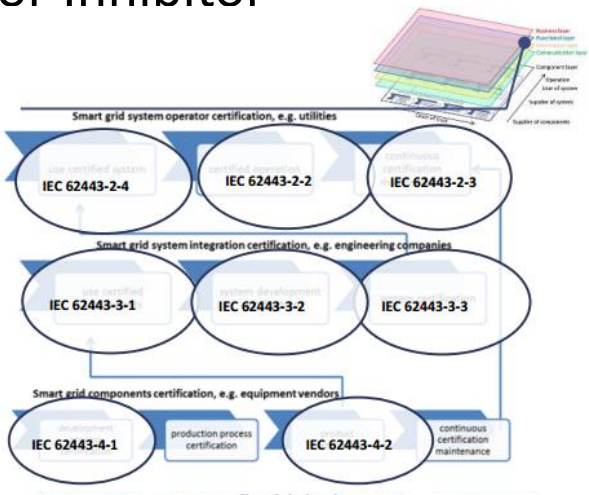
confer strength in numbers

intelworks LAUNCHING SUMMER 2015

SOLTRA

Source : LSEC 2015

Innovator Inhibitor



Source : ENISA, Smart Grid Security Certification in Europe, 01/2015

NOT THE END

These slides, more information and follow-up :

www.ipacso.eu

(connect & stay connected / activities / cspforum 2015)

www.lsec.eu

Q or C
Ulrich Seldeslachts
ulrich@lsec.eu
+32 475 71 3602