Club R2GS

Club de Réflexion et de Recherche
en Gestion opérationnelle de la Sécurité

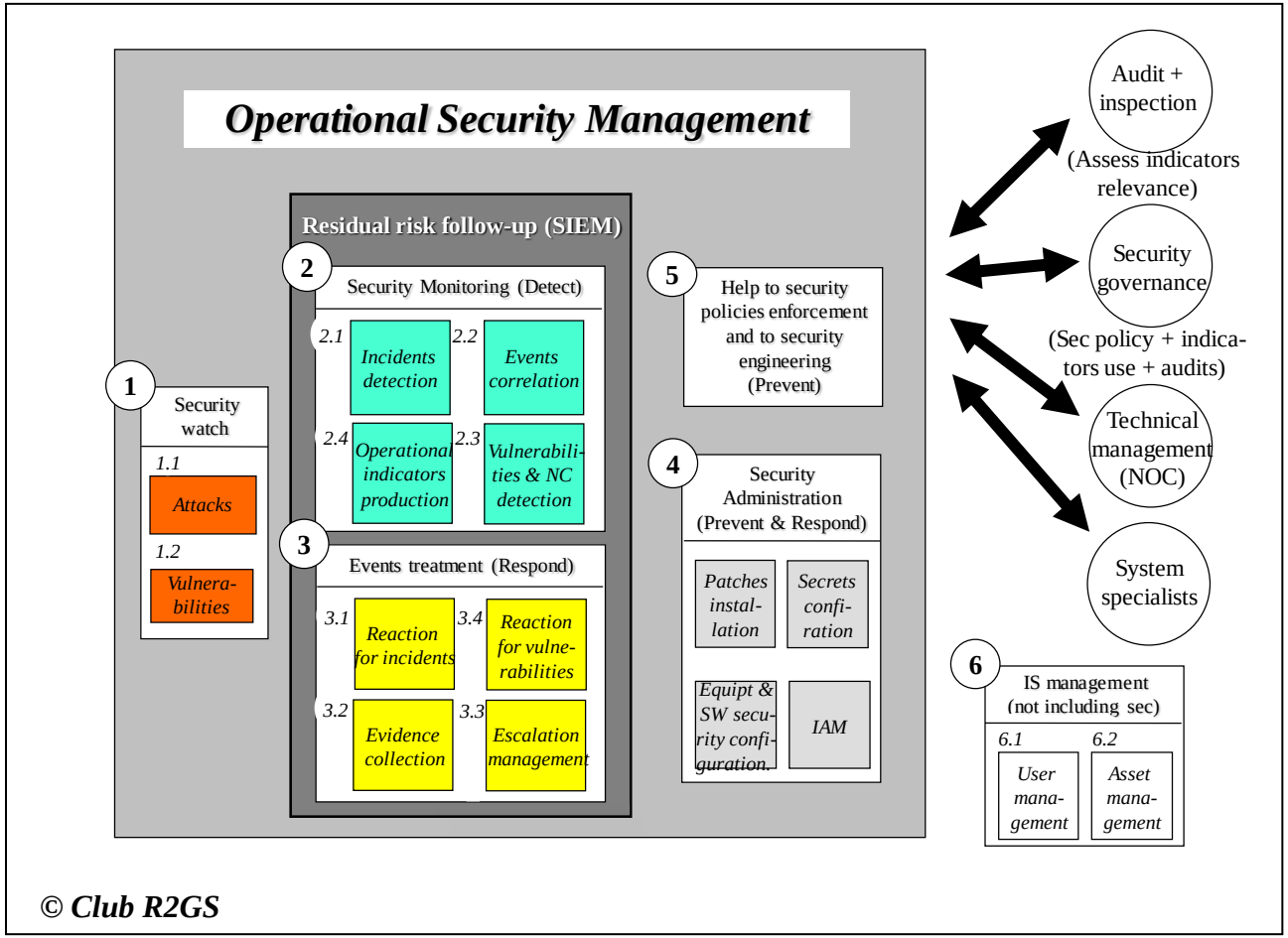
Club R2GS France and the European network of Chapters with their objectives and achievements

Gérard GAUDIN (G²C and Club R2GS France Chairman)

14 May 2014

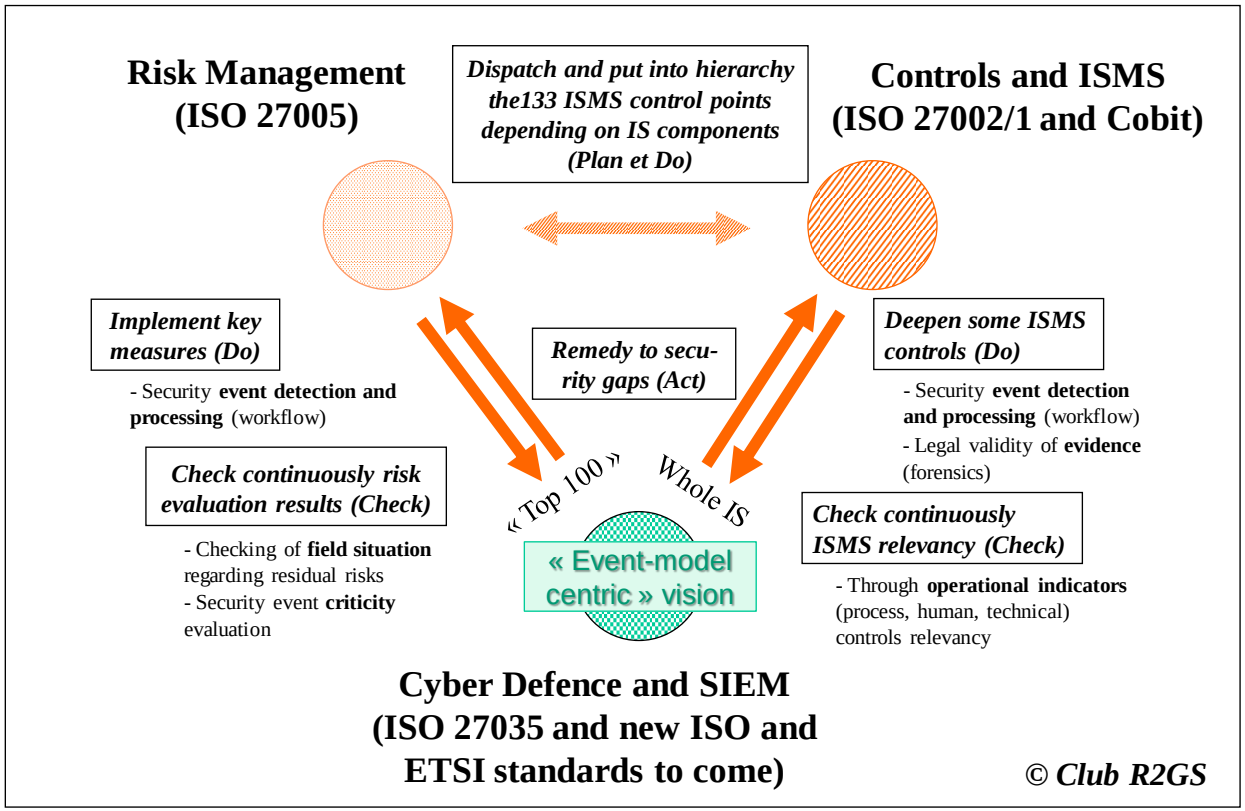
SUMMARY

1. Scope of Operational Security Management and Cyber Defense

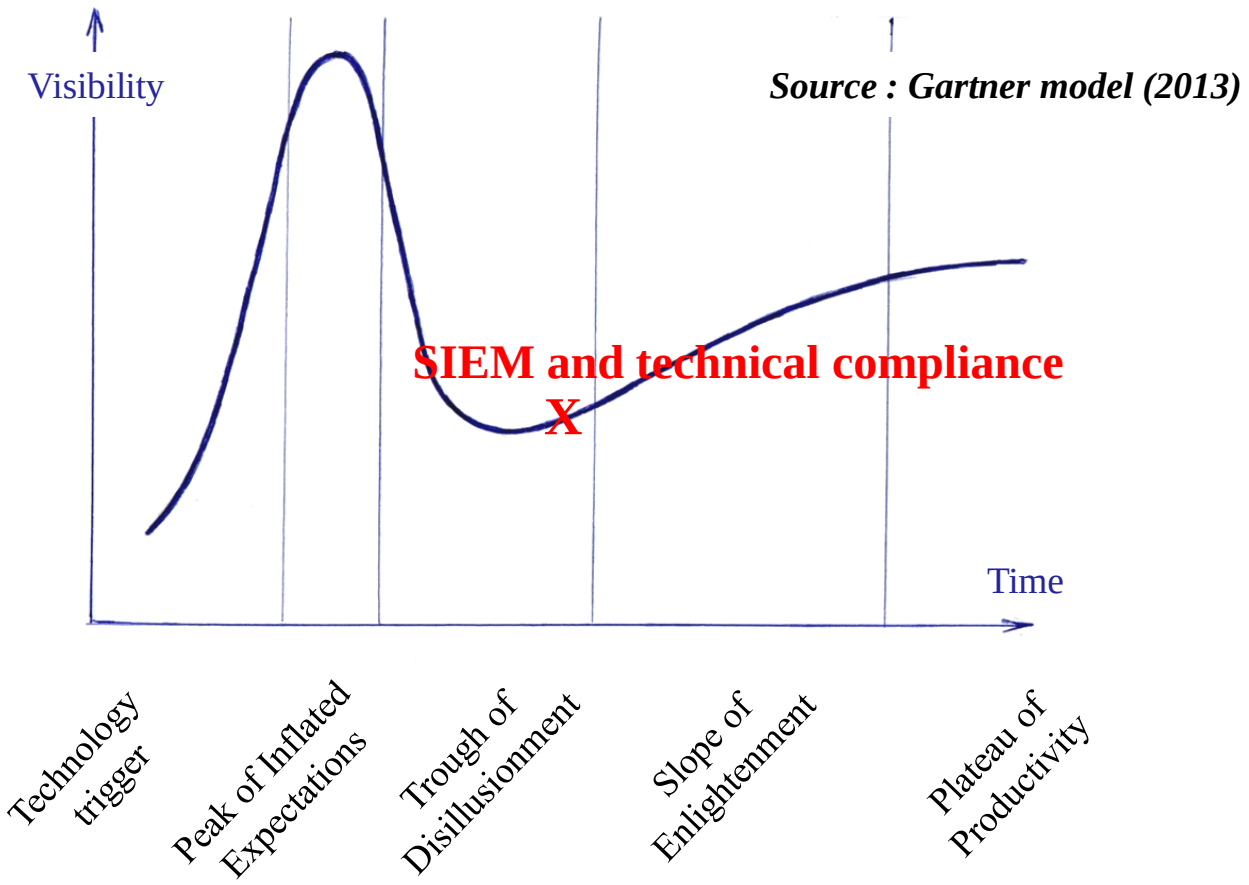


2. Positioning of the field

Real contribution only if positioned against the 2 root pillars



3. Status and maturity of the field



4. The Club R2GS Cyber Defense whole approach

Main directions

- Implement an approach with *4 key fulcrums and steps* =
  - ✓ Resting on 2 root pillars to define clear monitoring objectives (major risks, high frequency events – incidents & vulner./nonconformities)
  - ✓ Resting on a full set of models, reference frameworks and processes (contributing to work out continuous security assurance)
  - ✓ Streamline security investments and security operations based on statistical figures regarding incidents and vulnerabilities
  - ✓ Emphasis stressed on promoting the approach towards the whole organization (by demonstrating links with main IT business risks)
- 8 *organizational reference frameworks* are available (ISO 2700x compatible), cashing in on best practices, including =
  - ✓ 1st set (security event classification model, reference framework for indicators), both of them being subject to ETSI standardization
  - ✓ 2nd set (Needs expression guide to help SOC and internal « customers » work out a contract, reference framework for incident response plans)

5. Main results obtained (1)

*Key contribution of top-down and bottom-up approaches combination (organized around a set of some 100 operational indicators, which play a **key pivotal role** and are the **epitomy** of the approach)*

- Bring and *let work together* 2 different and often differing populations/interests (governance/technical & field experts) = « Indicators/Use cases » crossed analysis
- Detect events (incidents/vulnerabilities/nonconformities) that are *worth doing* (dangerousness or frequency)
  - ✓ Rarely the case in projects of the last 5 to 10 years
  - ✓ Best way to maintain pressure on organizations as regards security
- Upgrade often very low current event *detection rate* (even for the best ones)
  - ✓ 10 to 15 % for many incidents (most of the time by mere chance and long after their occurrence – Several days or weeks or months behind)
  - ✓ Only 6 % of data breaches are found out via logs (Verizon DBIR) – While evidence does exist in logs in 60 % of all cases

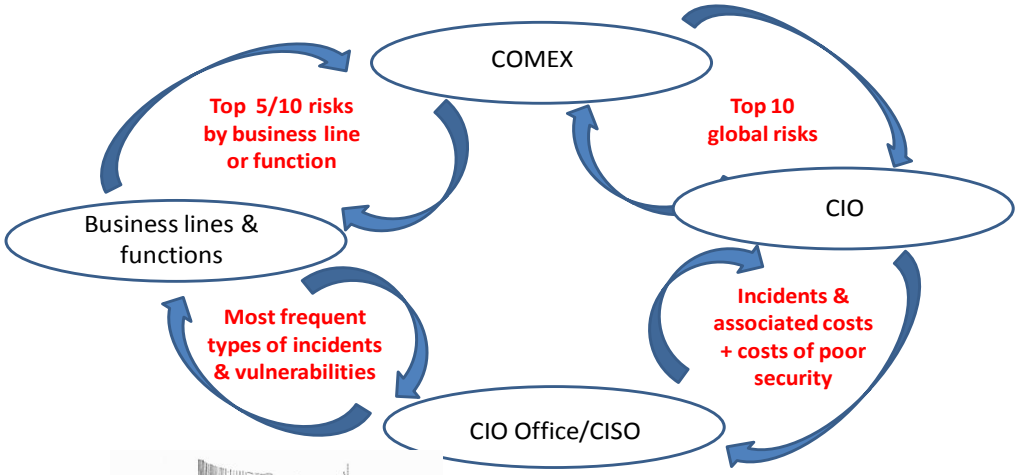
5. Main results obtained (2)

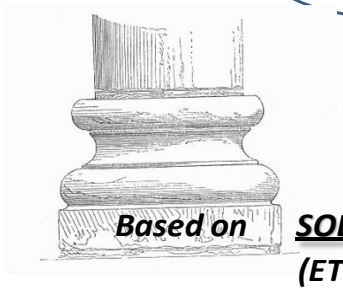
Position the proposed operational indicators against ISO 27002 controls = provide more assurance to governance and auditors

ISO 27002 control areas	ISO 27006 technical 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	x	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	x	IEX_PHY.1	VTC_PHY.1	Marginal topic for a SIEM approach
…	**…**	…	…	…
A15	**XX**	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

5. Main results obtained (3)

Heading towards a thorough and quantified knowledge of cyber risks and involve top management into cyber risks oversight to subsequently mobilize the whole comapny





SOLID INTELLIGENCE GROUNDINGS

(ETSI ISG ISI standards on security indicators)

5. Main results obtained (4)

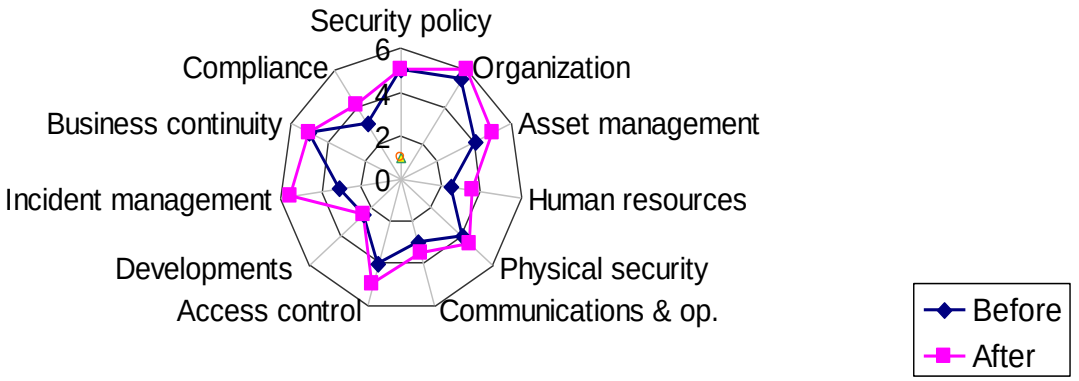
How to implement: first optimise the use of existing security equipment within company and don't forget to tackle « computer hygiene »

- Select according to different criteria *indicators and associated types of events* (incidents/vulnerabilities/nonconformities)
  - ✓ List of main types of security events (94)
  - ✓ Associated elements (in company context, notably based on Club R2GS experience and state-of-the-art figures) = occurrence likelihood, severity, types of assets concerned, types and levels of potential contribution and value (Risk mitigation/user awareness/regulatory compliance), methods/means of detection, complexity/effort of detection
  - ✓ Target production of 10 to 15 new indicators (notably with ISO 27002 or Cobit DS.5 correspondence)
- Potential of detection with existing means, often high (but under-used)
  - ✓ Ex. APTs (detected most of the time through network/system loads or outbound links)
  - ✓ Ex. Many behavioral nonconformities (can be detected via logs information available at the perimeter level)

5. Main results obtained (5)

As a summary, according to a Gartner study held in 2012 with 12 US organizations

Across the board security level (before and after a SIEM approach) - According the 11 ISO 27001 directions



5. Main results obtained (6)

Towards a quantitative vision of Cyber Security, assessed as other management disciplines (horizon of 3 to 5 years)

- *Shared indicators* broadly disseminated =
  - ✓ Precise measurement of ISMS effectiveness and of existing IT security controls
  - ✓ Measurement of security products effectiveness
  - ✓ Evaluation of awareness campaigns by in-depth knowledge of users' deviant behaviours
  - ✓ Working out of powerful compound indicators (for ex. C breach)
- Industry sector-specific and/or country-specific and/or European-wide databases (external or internal cybercrime, deviant behaviours, vulnerabilities)
- Possible *dependable and detailed continuous benchmarking* of organizations' security posture

5. Main results obtained (7)

Feasibility of a benchmarking approach demonstrated by G²C based on a international sample of companies in 4 countries

	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_ PHI.1	33 campaigns	Yes (only Fr & Ger)	100 % against state-of-the-art (between -70 % and +50 %)	1	Standard	Standard	RSA + complementary figures on typology	Quarterly
IEX_ DOS.1	0,008 DDoS attack	No	80 % against state-of-the-art (between -50 % and +50 %)	1	Standard	By Web site	CSI and sample of 15	Annual + quartterly tuning
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	CSI and sample of 15	Annual + quartterly tuning
VCF_ UAC.3	6 not compliant accounts	No	50 % against state-of-the-art (between -60 % et +40 %)	3	Standard	By database or application	Sample of 15	Quarterly

6. Club R2GS France Chapter overview (1)

What are we talking about ?

- Why a strong need to build a security community in this field exists (in most European countries) ?
  - ✓ Share security practices and the security situation regarding malicious (internal and external) attacks and deviant internal behaviours, and deepen the knowledge on this matter within a ***gathering of trust*** (what is lacking the most)
  - ✓ Be as organized as the attacker community
  - ✓ Complement the CERT/CSIRT community and the standardization bodies
- Structure the community around new standards (ETSI)
  - ✓ Operational indicators and Security event classification model especially
- Association based on this principles launched in France in 2009

6. Club R2GS France Chapter overview (2)

A complete set of complimentary key players

- Users involved in Cyberdefense/SIEM approaches within their organizations (with more or less big technical investments), representing the various industry sectors (including critical infrastructure)
- Institutional members (ANSSI, European Commission, …)
- Vendors covering the whole IT security field =
  - ✓ G²C (Consulting in IT security specializing in Cyberdefense and SIEM, and provider with key statistical state-of-the-art figures)
  - ✓ CEIS (Consulting in strategic intelligence and in safety)
  - ✓ Alcatel-Lucent (MSSP and SIEM system integration)
  - ✓ Airbus Cybersecurity (MSSP and SIEM system integration)
  - ✓ Atos (Consulting and system integration)
  - ✓ Caprioli & Associés (Consulting in the legal field linked to Cybersecurity)

6. Club R2GS France Chapter overview (3)

List of members – 43 large organizations and 200 individuals

Airbus Defense & Space Cybersecurity
Air France KLM
Alcatel-Lucent
Allianz
ANSSI (IT Security government agency)
Atos Origin
BNP Paribas
Bouygues Construction
Bouygues Telecom
Caisse des Dépôts et Consignations
Caprioli & Associés
CEA
CEIS
Cert IST
CNAMTS
Crédit Agricole
EDF
European Commission
G²C
Groupama
Groupement des Cartes Bancaires CB
Humanis
Informatique Banques Populaires (i-BP)
La Française des Jeux
La Poste
Ministère de l'Agriculture
Ministère de la Défense
Ministère de l'Économie et des Finances
Ministère de l'Éducation Nationale
Ministère de l'Intérieur/Gendarmerie Nat.
Ministère de l'Intérieur
Ministère de la Justice
Ministère de la Santé et des Sports
Natixis
Oppida
Orange
Premier Ministre
PSA Peugeot Citroën
Renault
SFR
Société Générale
ST Microelectronics
Telecom Paris Tech

6. Club R2GS France Chapter overview (4)

Summary of documents produced and results obtained since 2009

- Working Groups (7 completed or underway)
- « Matinales » - Cf. dedicated workshops and exchanges with experienced experts or user organisations (10 achieved in 5 years)
- Cyber Defense and SIEM annual unique gathering called « Les Assises du domaine Cyber Défense et SIEM » (open to the whole profession in France)
  - ✓ 160 participants on the 4th one held in 2013 (with the participation of Club R2GS France/UK/Germany/Luxemburg heads)
- Annual Ordinary General meetings (5 already held)
- Turn the Chapter into a Cyber Defense Observatory (with periodic collection of *state-of-the art statistical figures* in line with ETSI GS ISI-001 on Indicators) = study underway

7. The European network of Chapters