9th International Cybersecurity Forum

FIC 2017

24TH & 25TH OF JANUARY 2017 | LILLE GRAND PALAIS

Which operational indicators for efficient SOCs and a robust Cyber defense ?

(Workshop A19)

Club R2GS

Smarter security for future technologies

SPEAKERS

Gerard Gaudin, Independent international consultant G²C, Head of Club R2GS France and Europe **– *Moderator***

Christophe Bianco, Managing Partner of Excellium Services, and Head of Club R2GS Luxembourg

Jan deMeer, CEO smartspacelabs.eu, and Head of Club R2GS Germany

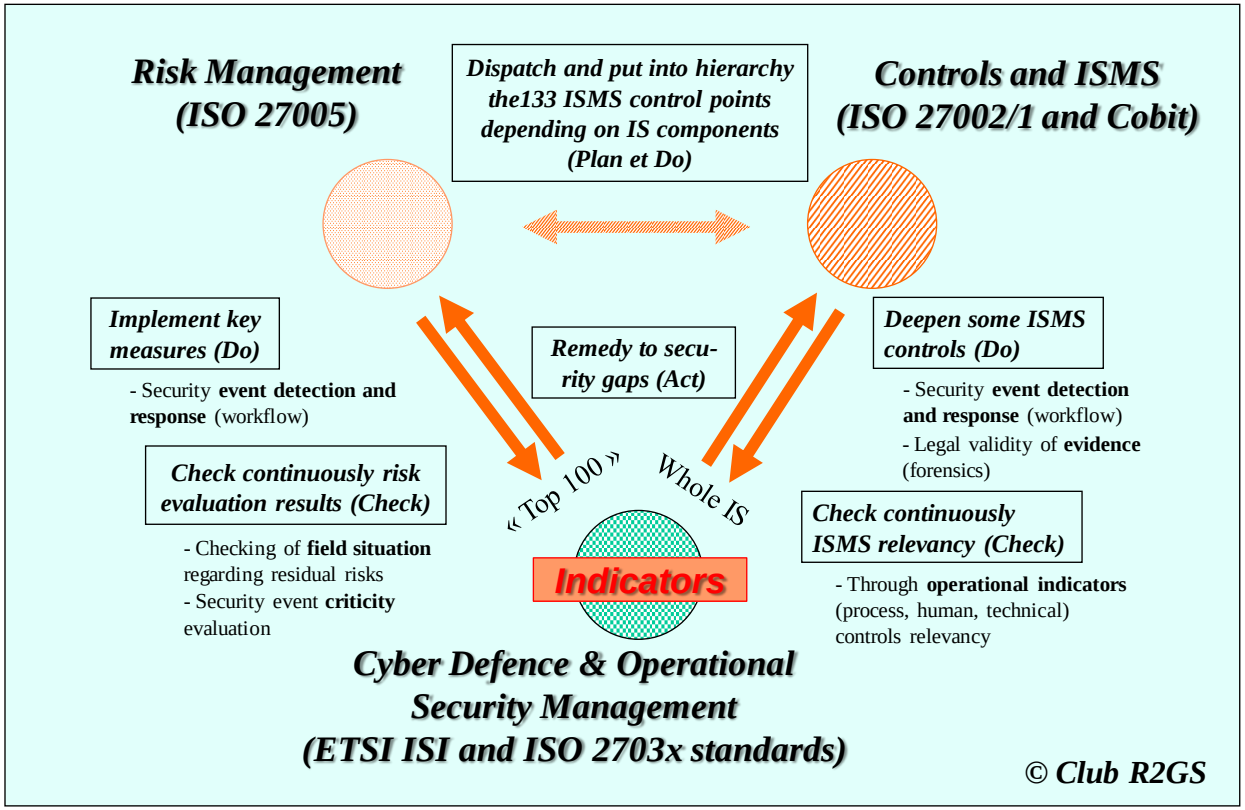
Yann Leborgne, South Europe Pre-sales manager of ThreatQuotient

Marc Leymonerie, Air France KLM Group CISO

Cedric Manca, Exaprobe IT Security Manager

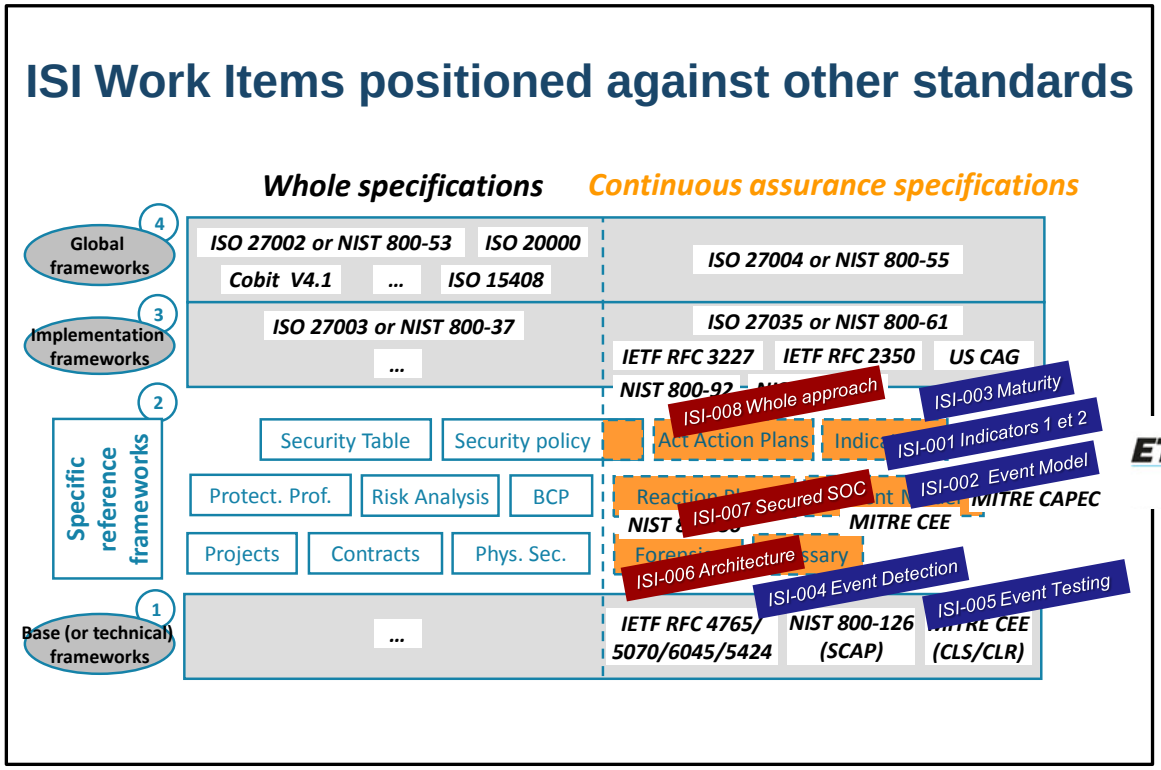
Field and topics positioning

Real contribution only if positioned against the 2 root pillars



A whole approach at the crossroads of governance and technical expertise

A standardized approach filling a gap in the incident detection standardization field (ETSI ISI)



Many diversified uses

How to use ETSI GS ISI-001 indicators in various manners: 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

Lower level

– **4.** Human resources and management

– **5.** IT Operations and Production executives

– **6.** IT Engineering executives

B. ***Stimulate exchanges within the profession*** (further to the ones found in existing 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 (LPM, NIS Directive, GDPR,…

Richness of uses demonstrated

Gerard Gaudin, Introduction and workshop presentation

Marc Leymonerie, Mobilize an overall company with progress in user behaviour

Christophe Bianco, Measuring the effectiveness of a SOC

Cedric Manca, Measuring the effectiveness of a SOC

Yann Leborgne, Threat intelligence contribution to incident detection

Jan deMeer, Extending usual Cybersecurity to monitoring of industrial systems

Richness of uses demonstrated

Gerard Gaudin, Introduction and workshop presentation

Marc Leymonerie, Mobilize an overall company with progress in user behaviour

Christophe Bianco, Measuring the effectiveness of a SOC

Cedric Manca, Measuring the effectiveness of a SOC

Yann Leborgne, Threat intelligence contribution to incident detection

Jan deMeer, Extending usual Cybersecurity to monitoring of industrial systems

Richness of uses demonstrated

Gerard Gaudin, Introduction and workshop presentation

Marc Leymonerie, Mobilize an overall company with progress in user behaviour

Christophe Bianco, Measuring the effectiveness of a SOC

Cedric Manca, Measuring the effectiveness of a SOC

Yann Leborgne, Threat intelligence contribution to incident detection

Jan deMeer, Extending usual Cybersecurity to monitoring of industrial systems

Richness of uses demonstrated

Gerard Gaudin, Introduction and workshop presentation

Marc Leymonerie, Mobilize an overall company with progress in user behaviour

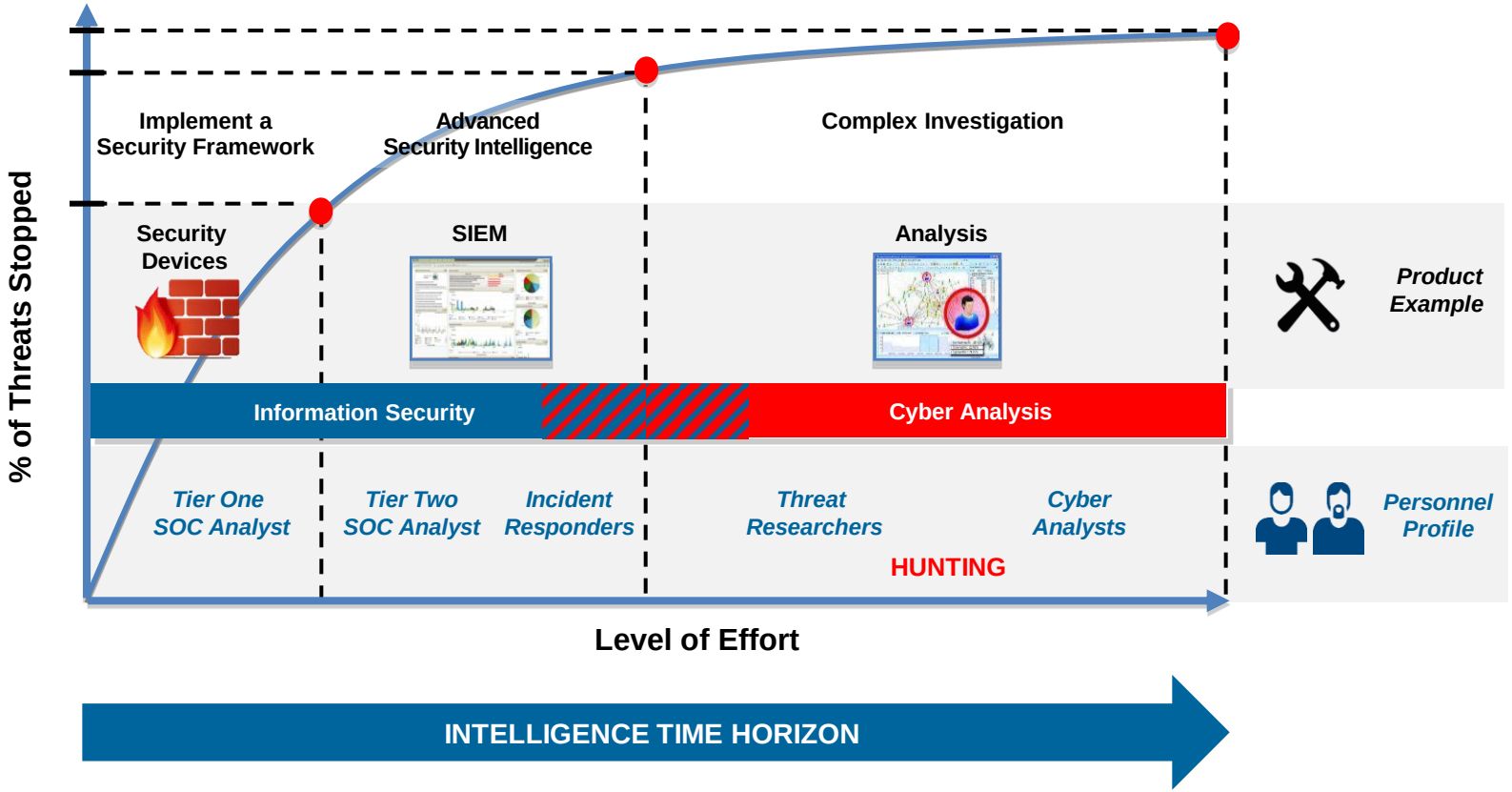
Christophe Bianco, Measuring the effectiveness of a SOC

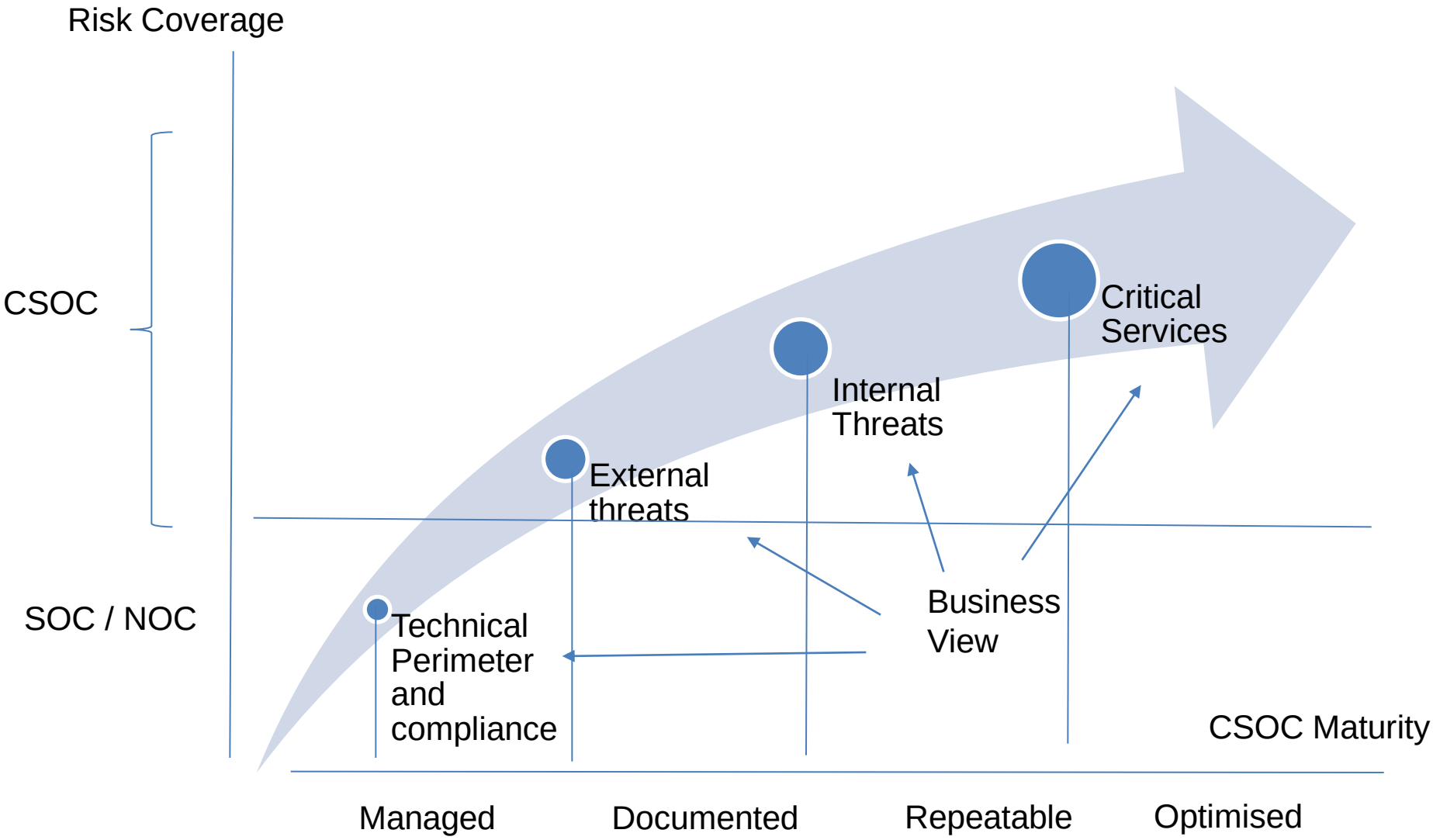
Cedric Manca, Measuring the effectiveness of a SOC

Yann Leborgne, Threat intelligence contribution to incident detection

Jan deMeer, Extending usual Cybersecurity to monitoring of industrial systems

Non-Linear Relationship Between Effectiveness and Cost




Risk Coverage
CSOC
SOC / NOC
Critical Services
Internal Threats
External threats
Technical Perimeter and compliance
Business View
CSOC Maturity
Managed
Documented
Repeatable
Optimised

Richness of uses demonstrated

Gerard Gaudin, Introduction and workshop presentation

Marc Leymonerie, Mobilize an overall company with progress in user behaviour

Christophe Bianco, Measuring the effectiveness of a SOC

Cedric Manca, Measuring the effectiveness of a SOC

Yann Leborgne, Threat intelligence contribution to incident detection

Jan deMeer, Extending usual Cybersecurity to monitoring of industrial systems

Richness of uses demonstrated

Gerard Gaudin, Introduction and workshop presentation

Marc Leymonerie, Mobilize an overall company with progress in user behaviour

Christophe Bianco, Measuring the effectiveness of a SOC

Cedric Manca, Measuring the effectiveness of a SOC

Yann Leborgne, Threat intelligence contribution to incident detection

Jan deMeer, Extending usual Cybersecurity to monitoring of industrial systems

Richness of uses demonstrated

Gerard Gaudin, Introduction and workshop presentation

Marc Leymonerie, Mobilize an overall company with progress in user behaviour

Christophe Bianco, Measuring the effectiveness of a SOC

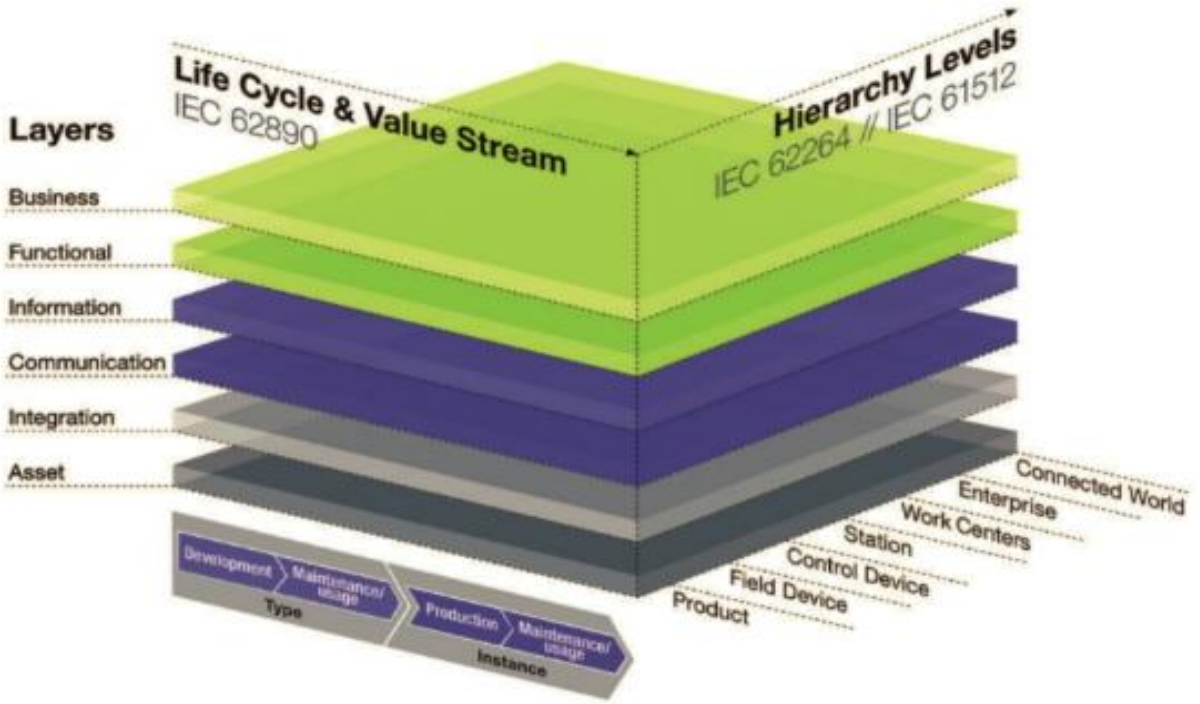
Cedric Manca, Measuring the effectiveness of a SOC

Yann Leborgne, Threat intelligence contribution to incident detection

Jan deMeer, Extending usual Cybersecurity to monitoring of industrial systems

Extending usual Cybersecurity to monitoring of industrial systems

- Q0:

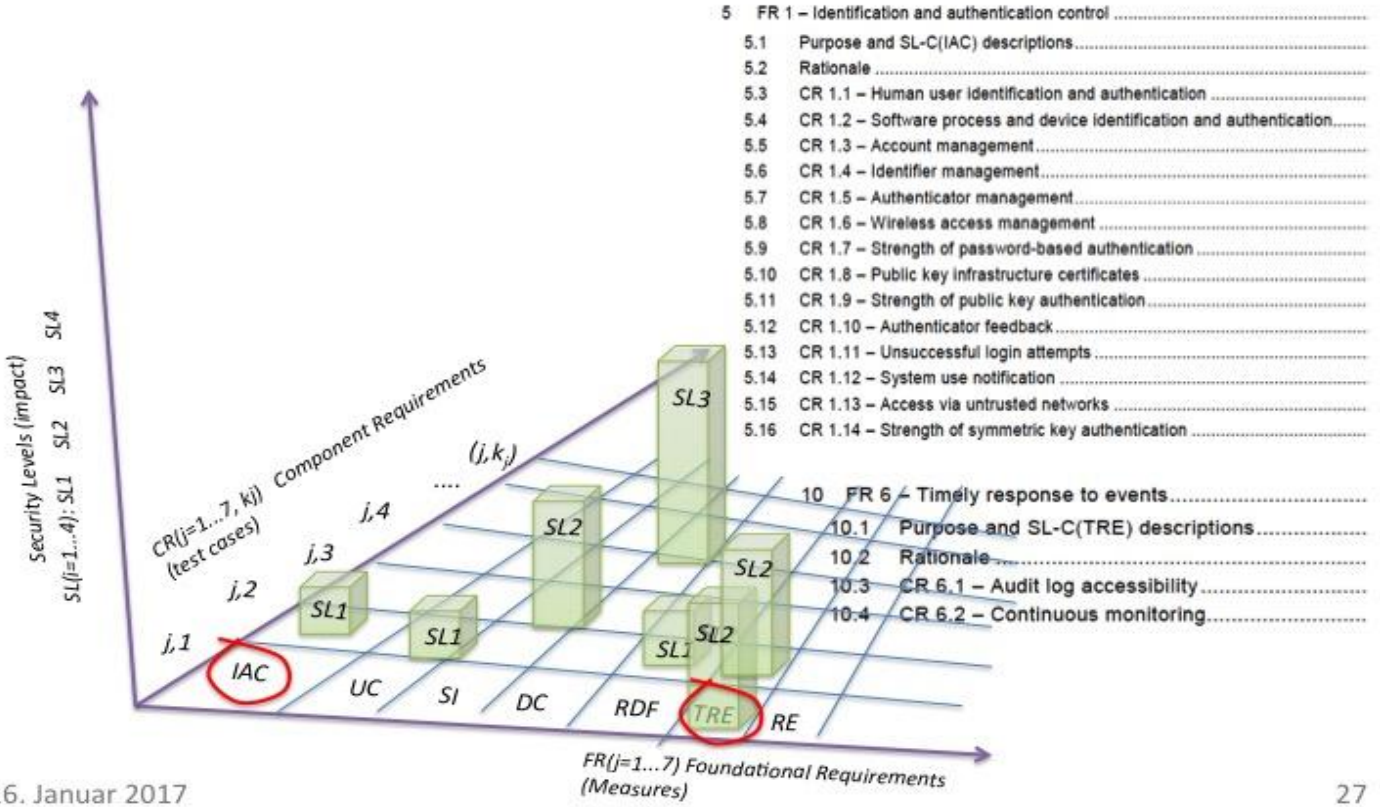


Das Referenzarchitekturmodell RAMI 4.0
© Plattform Industrie 4.0

Extending usual Cybersecurity to monitoring of industrial systems

- Q1:

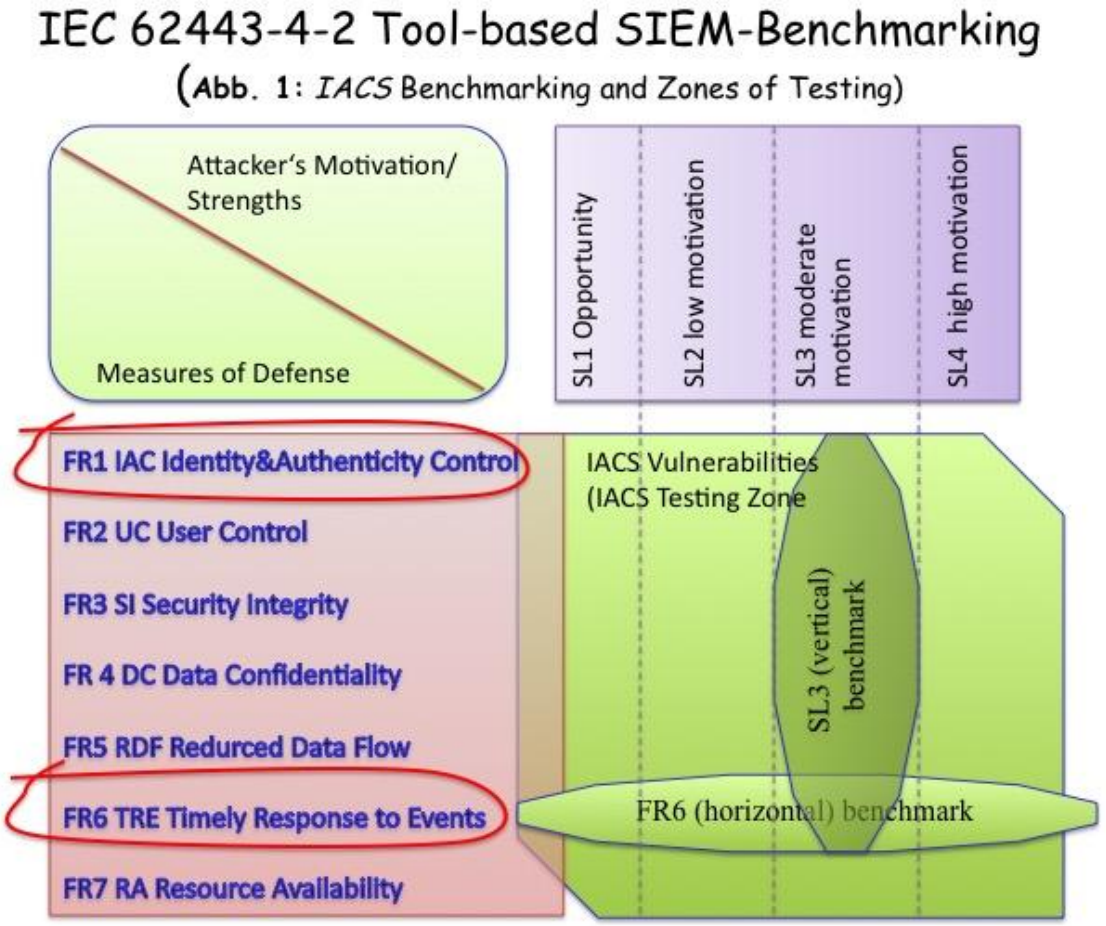
IEC 62443-4-2 Dimensions of SIEM-Benchmarking
(Abb. 2: CR Benchmarking part of *SIEM* Landscape)



FIC 2017
24 & 25 JANVIER 2017 | LILLE GRAND PALAIS
Club R2GS

Extending usual Cybersecurity to monitoring of industrial systems

Q2:



FIC 2017
24 & 25 JANVIER 2017 | LILLE GRAND PALAIS
Club R2GS

Extending usual Cybersecurity to monitoring of industrial systems

Q3: