Security in knowledge

Cyber Security Information Exchange

Luc Dandurand

NATO Communications and Information Agency

RSA®CONFERENCE
EUROPE 2013

Session ID: SECT-T08

Session Classification: General Interest

Overview

- Cyber security in NATO
- Highlight of existing efforts and solutions
- Challenges still affecting information sharing
- The Cyber Security Data Exchange and Collaboration Infrastructure (CDXI):
  - High-Level Requirements
  - Deployment and Integration
  - Knowledge Markets
  - Agile Data Model
  - Enabling Automation
  - Support for Commercial Exploitation

Cyber Security In NATO

Security in knowledge

#RSAC

RSA CONFERENCE
EUROPE 2013

Cyber Security In NATO

- NATO in a nutshell:
  - Collective defence
  - Interoperable capabilities
  - Policies for sharing information
  - NATO has its own systems to protect
  - NATO relies on National systems for its missions and operations
- NATO's 2010 Strategic concept
  - Cyber security is a key concern
- NATO Computer Incident Response Capability (NCIRC)
  - Coordination Centre (CC)
  - Technical Centre (TC)
- Annual Cyber Coalition Exercise

Highlight of Existing Efforts and Solutions

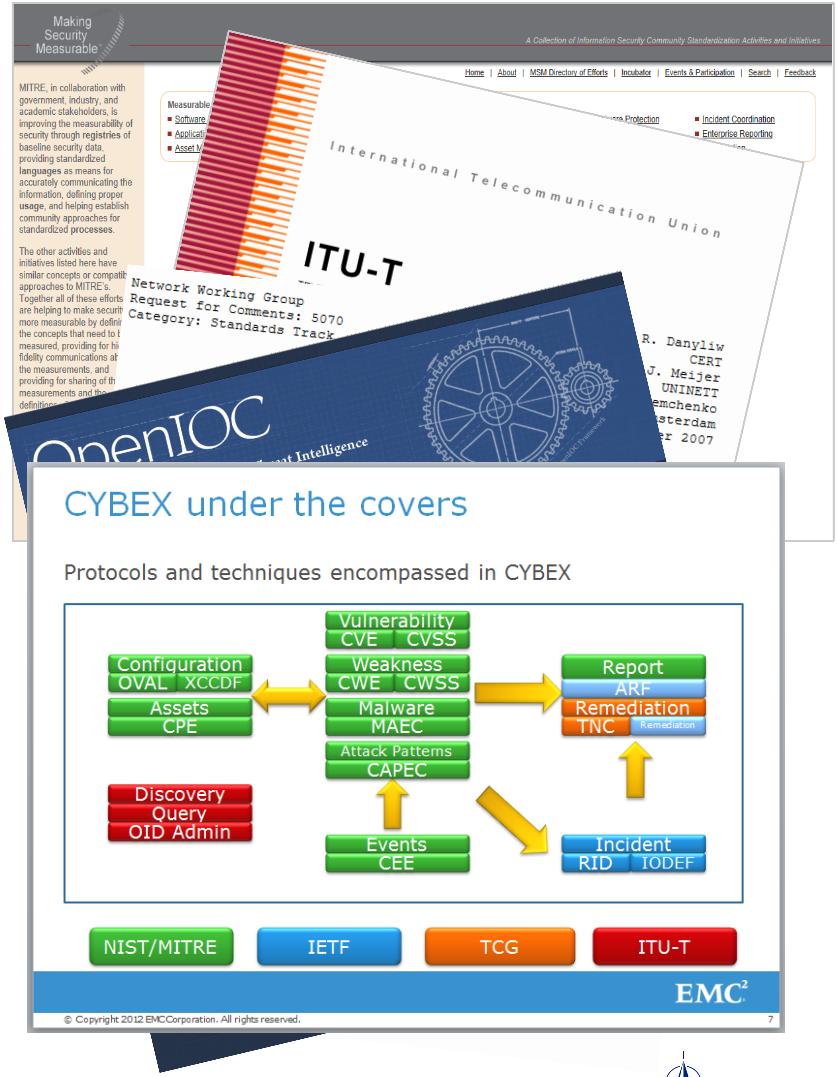
Security in knowledge

#RSAC

RSA CONFERENCE
EUROPE 2013

Standardization Efforts

- Standards:
  - US Govt / MITRE's "Making Security Measurable" program
  - ITU-T's X.1500 CYBEX
  - IETF's Incident Object Description and Exchange Format (IODEF) and Real-time Inter-network Defence (RID)
  - Vendor Formats
    - Proprietary or Open source
- Most are interoperable!



Making Security Measurable™

A Collection of Information Security Community Standardization Activities and Initiatives

Home | About | MSM Directory of Efforts | Incubator | Events & Participation | Search | Feedback

MITRE, in collaboration with government, industry, and academic stakeholders, is improving the measurability of security through **registries** of baseline security data, providing standardized **languages** as means for accurately communicating the information, defining proper **usage**, and helping establish community approaches for standardized **processes**.

The other activities and initiatives listed here have similar concepts or compatib approaches to MITRE's. Together all of these efforts are helping to make securit more measurable by defini the concepts that need to b measured, providing for hi fidelity communications ab the measurements, and providing for sharing of th measurements and the definition

Measurable
- Software
- Applicati
- Asset M
- re Protection
- Incident Coordination
- Enterprise Reporting

International Telecommunication Union

ITU-T

Network Working Group
Request for Comments: 5070
Category: Standards Track

R. Danyliw
CERT
J. Meijer
UNINETT
emchenko
sterdam
er 2007

OpenIOC

at Intelligence

CYBEX under the covers

Protocols and techniques encompassed in CYBEX

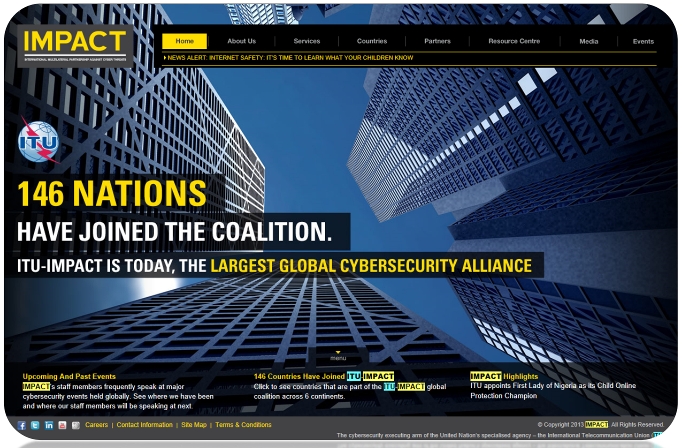
EMC²

© Copyright 2012 EMC Corporation. All rights reserved.

7

Existing Capabilities

- Platforms / Systems / Services:
  - Information Sharing and Analysis Centres (ISACs)
  - Resiliency and Security Forum of the Internet Systems Consortium
  - Multinational Alliance for Collaborative Cyber Situational Awareness (MACCSA)
  - Collective Intelligence Framework (CIF)
  - ITU's IMPACT
  - NATO's Malware Information Sharing Platform (MISP)
- Many efforts in other domains (e.g. bioinformatics)



IMPACT

INTERNATIONAL MULTILATERAL PARTNERSHIP AGAINST CYBER THREATS

Home | About Us | Services | Countries | Partners | Resource Centre | Media | Events

NEWS ALERT: INTERNET SAFETY: IT'S TIME TO LEARN WHAT YOUR CHILDREN KNOW

ITU

146 NATIONS

HAVE JOINED THE COALITION.

ITU-IMPACT IS TODAY, THE LARGEST GLOBAL CYBERSECURITY ALLIANCE

menu

Upcoming And Past Events
IMPACT's staff members frequently speak at major cybersecurity events held globally. See where we have been and where our staff members will be speaking at next.

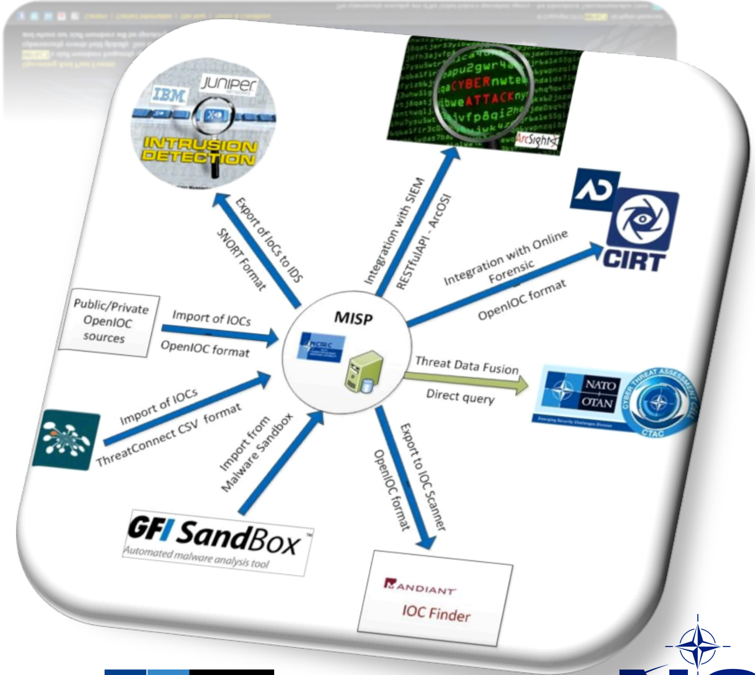
146 Countries Have Joined ITU-IMPACT
Click to see countries that are part of the ITU-IMPACT global coalition across 6 continents.

IMPACT Highlights
ITU appoints First Lady of Nigeria as its Child Online Protection Champion

Careers | Contact Information | Site Map | Terms & Conditions

© Copyright 2013 IMPACT. All Rights Reserved.

The cybersecurity executing arm of the United Nation's specialised agency – the International Telecommunication Union (ITU)



MACCSA
Ensuring access to cyberspace

Challenges Affecting Information Sharing in Cyber Security

Security in knowledge

#RSAC

RSA CONFERENCE
EUROPE 2013

Challenges (1/2)

- Developing models for complex realities
- Lots of data sources available in the public domain, leading to information overload
- Timeliness requirement competes with quality requirement
- Multi-lateral, differentiated sharing is a requirement

Challenges (2/2)

- Sensitive data requires dissemination controls
- Poor quality and current data management approaches significantly limit automation
- Current processes and technologies do not support burden-sharing collaboration and outsourcing
- No direct financial benefit

➡ **Ongoing efforts must be continued, but they must also be complemented !**

Addressing the Challenges…

- Previous efforts have looked at how to exchange information between parties without much consideration for the internal problems for handling the exchanged data…
- In cyber security, there are many challenges in the management and exploitation of exchanged data…
- In cyber security, these challenges are mostly common to all…

- **Shouldn't we consider a common solution???**

CDXI:
A Cyber Security Information Exchange Platform

Security in knowledge

#RSAC

RSA® CONFERENCE
EUROPE 2013

CDXI Overview

- CDXI capability has 3 objectives:
  - Facilitate information sharing
  - Enable automation
  - Facilitate the generation, refinement and vetting of cyber security data through burden-sharing collaboration and outsourcing

- Focused on structured cyber security data

- **Share, automate and collaborate**

High-Level Requirements

HLR #1: Provide a flexible, scalable, secure and decentralized infrastructure based on freely available software

HLR #2: Provide for the controlled evolution of the syntax and semantics of multiple independent data models and their correlation

HLR #3: Securely store both shared and private data

HLR #4: Provide for customizable, controlled multilateral sharing

HLR #5: Enable the exchange of data across non-connected domains

HLR #6: Provide human and machine interfaces

HLR #7: Provide collaboration tools that enable burden sharing on the generation, refinement, and vetting of data

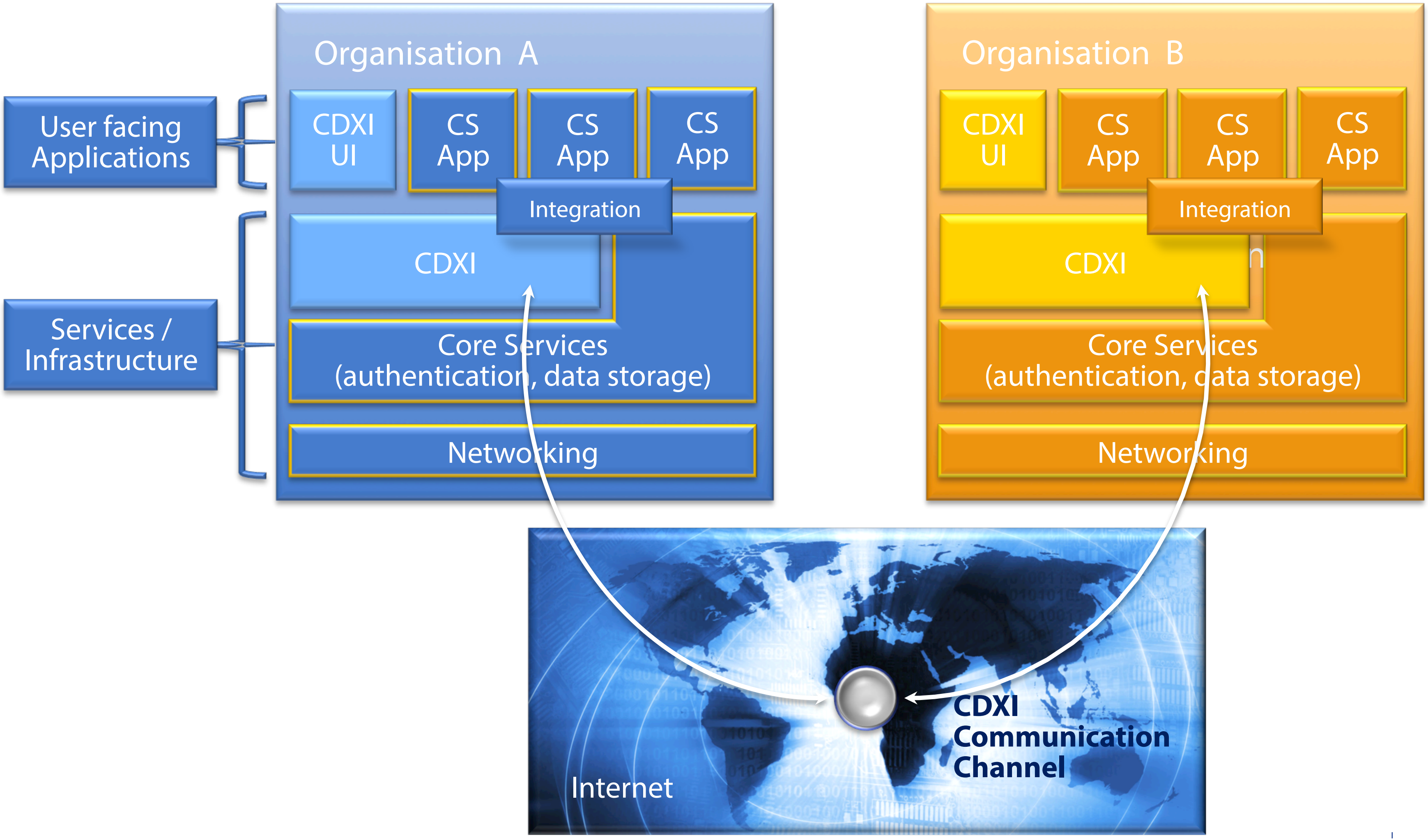
HLR #8: Provide customizable quality-control processes

HLR #9: Expose dissension to reach consensus

HLR #10: Support continuous availability of data

HLR #11: Enable commercial activities

Deployment and Integration



User facing Applications

Services / Infrastructure

Organisation A

CDXI UI

CS App

CS App

CS App

Integration

CDXI

Core Services (authentication, data storage)

Networking

Organisation B

CDXI UI

CS App

CS App

CS App

Integration

CDXI

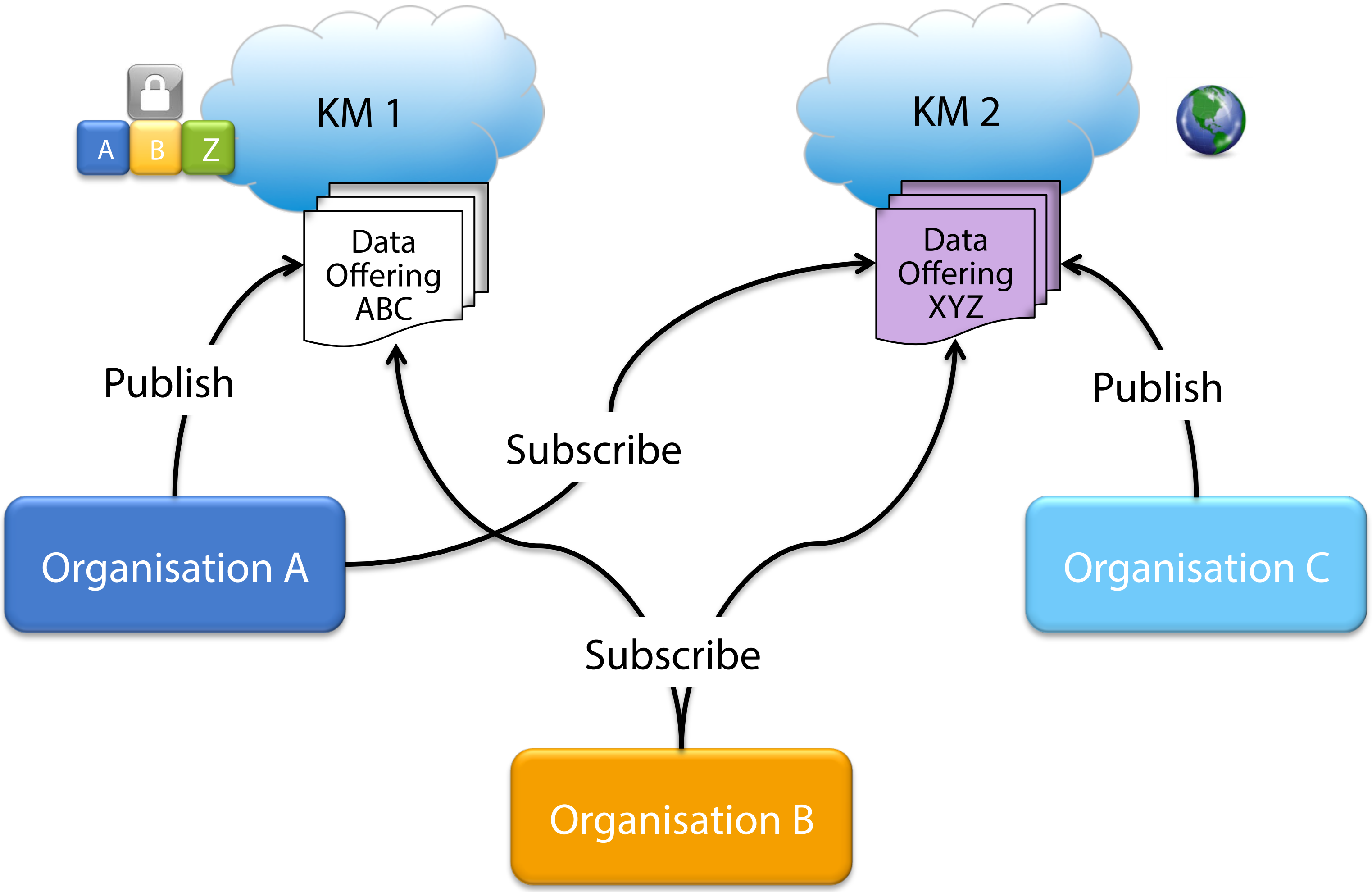
Core Services (authentication, data storage)

Networking

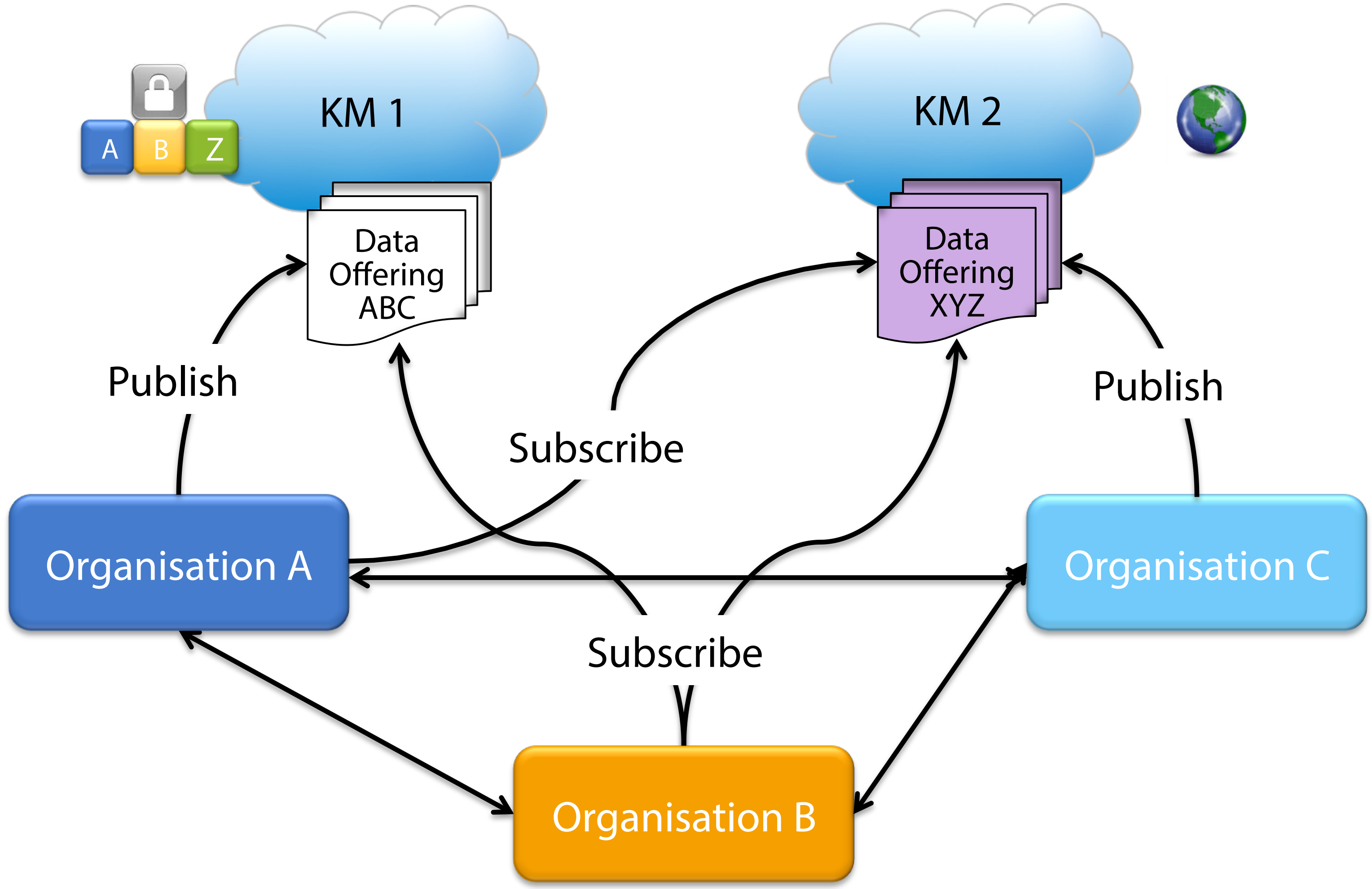
Internet

CDXI Communication Channel

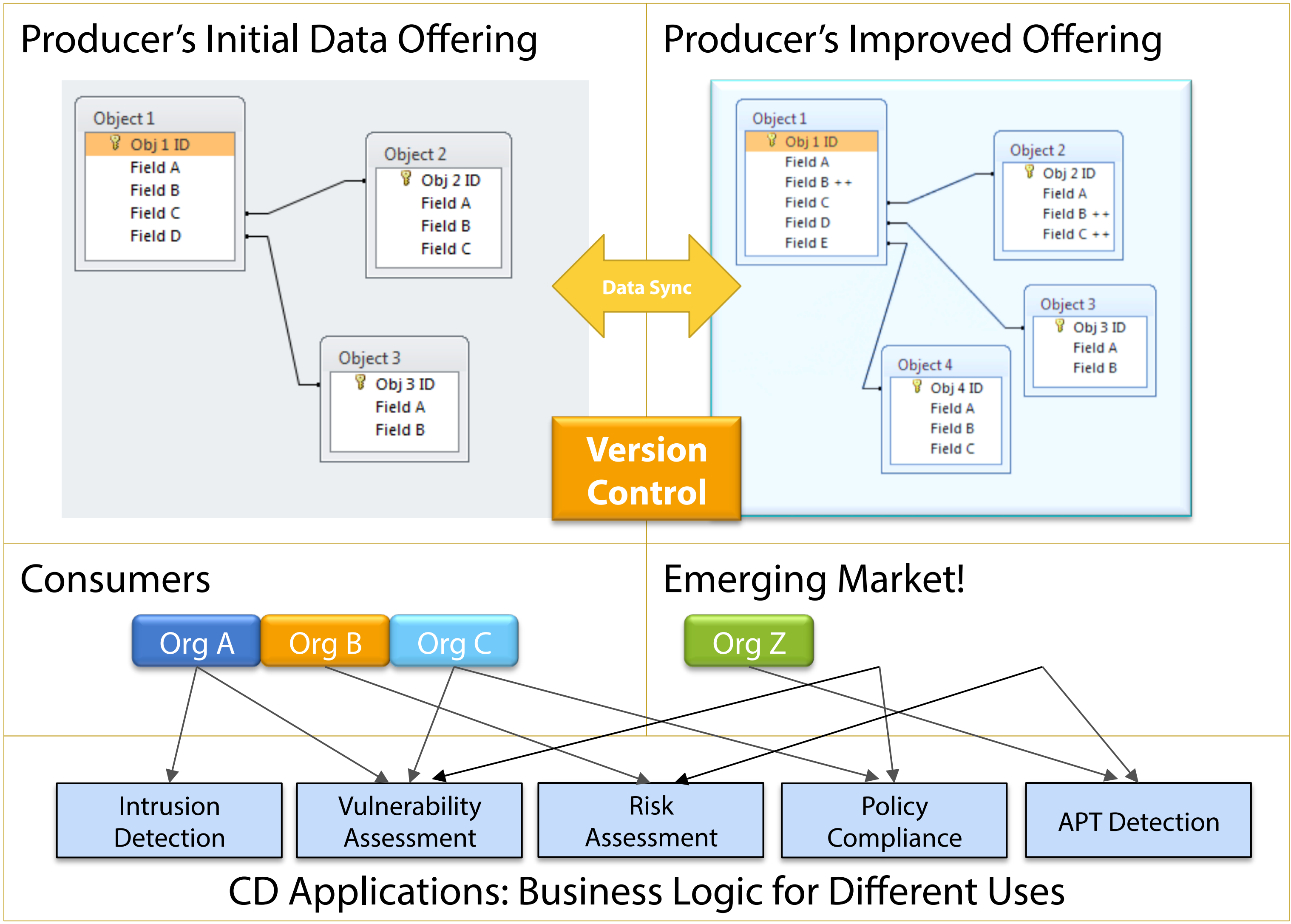
Knowledge Markets



Knowledge Markets



Agile Data Model



Producer's Initial Data Offering

Producer's Improved Offering

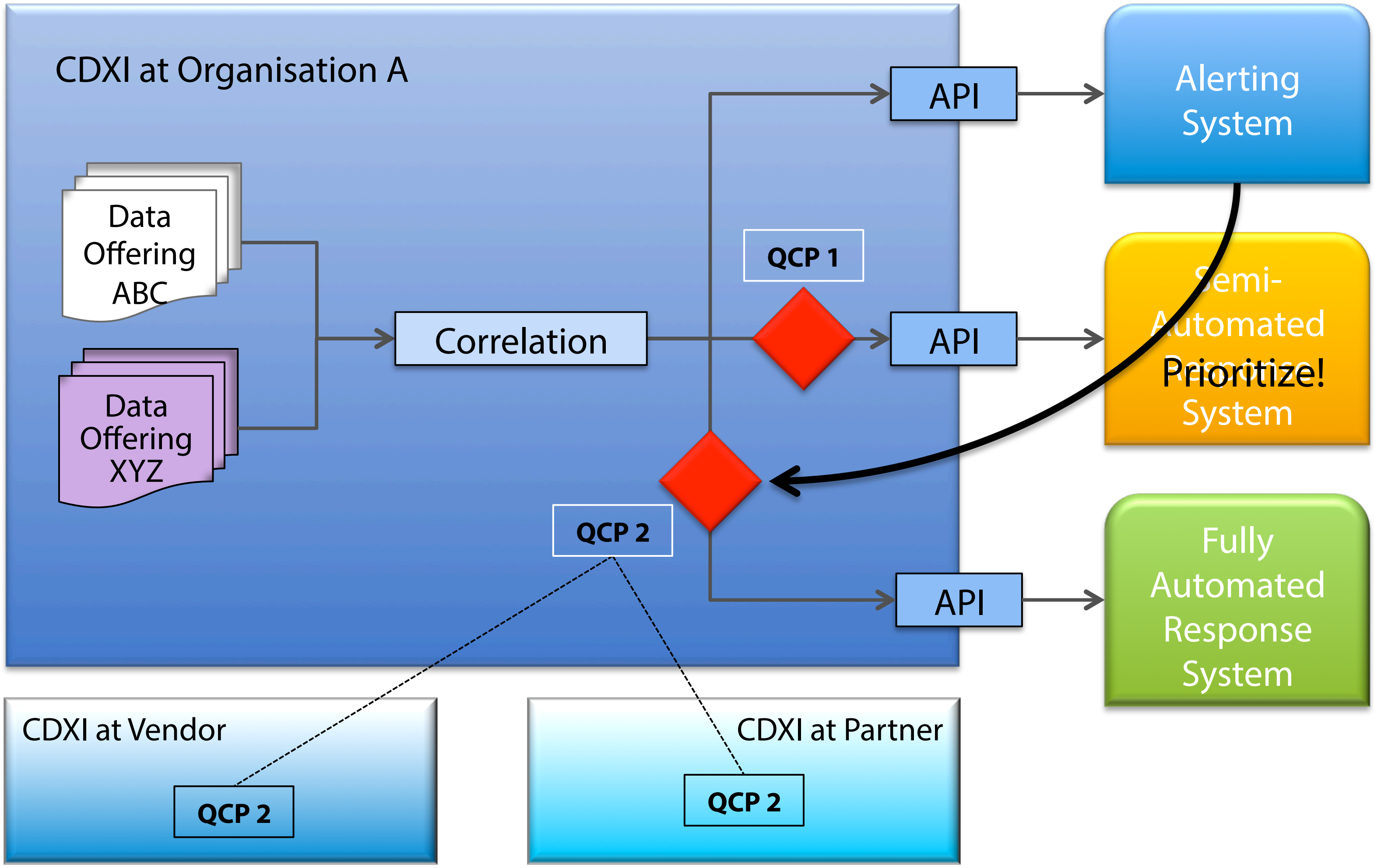
Version Control

Consumers

Emerging Market!

CD Applications: Business Logic for Different Uses

Enabling Automation

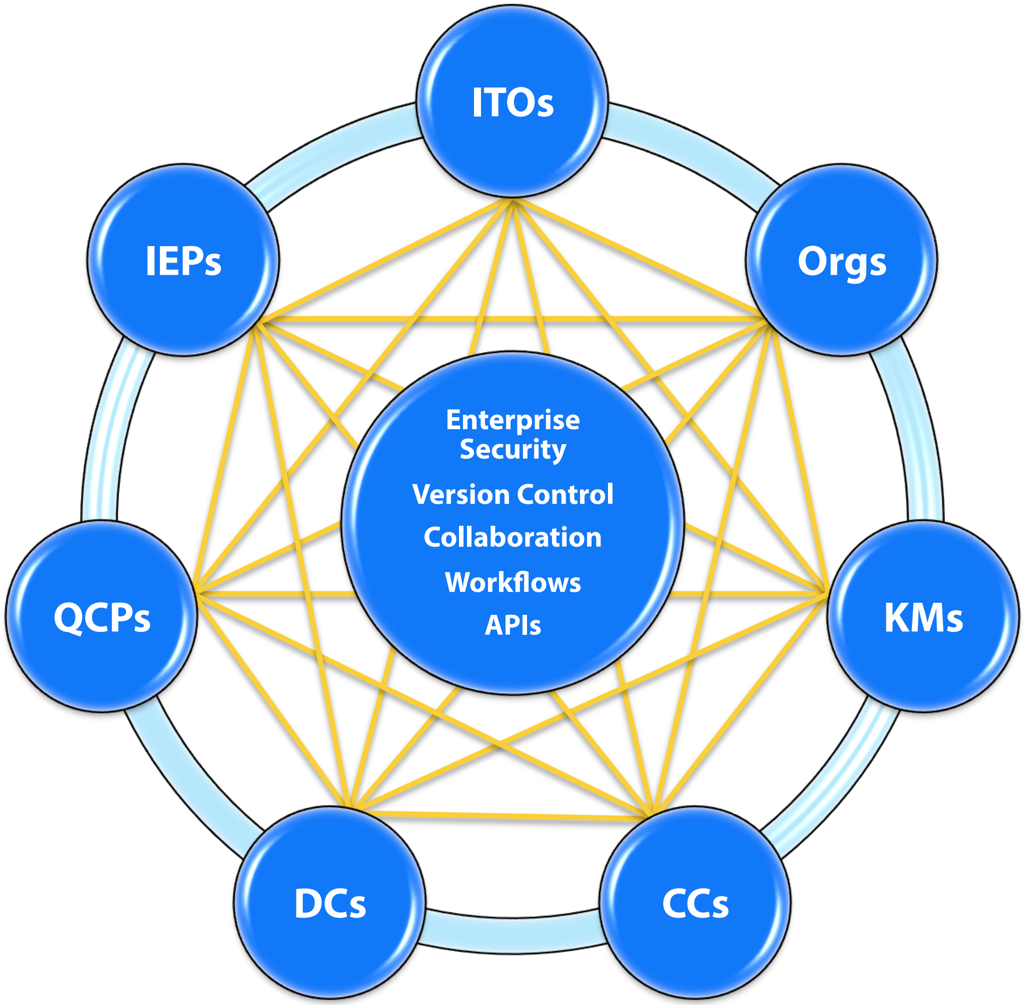


Support for Commercial Exploitation

- Enable easy accounting of exchange and use of information
- Support different business models, e.g.:
  - Pay a monthly fee for receiving continually updated data
  - Remote queries into a database, and "buy" a subset of records found
  - Only pay for records used to support automated processes
- Accounting for data-related services, e.g.:
  - Correlation of data sources
  - Quality assurance of data
  - Translation of data
- Can also be used to derive value metrics

Core Elements of CDXI

- Independent Topic Ontologies
- Information Exchange Policies
- Participating Organizations
- Quality Control Processes
- Communication Channels
- Knowledge Markets
- Digital Curations



Conclusion

- CDXI is a knowledge management platform specifically designed to address the information sharing issues of the Cyber Security domain
- NATO is seeking feedback on the proposed capability
  - If freely available, would you provide data accessible to NATO?
- CDXI implementation will be considered by NATO Nations in 2014
- Possible collaboration on refining use cases in 2014:
  - ACT: Mario Beccia (Mario.Beccia@act.nato.int)
  - NCIA: Luc Dandurand (Luc.Dandurand@ncia.nato.int)

Security in knowledge

Thank you!

Luc Dandurand

NATO Communications and
Information Agency

luc.dandurand@ncia.nato.int

www.ncia.nato.int