NATO Communications and Information Agency

Understanding CSIRT Knowledge Management Needs

Oscar Serrano

03 April 2013

Disclaimer

This work was sponsored by NATO's Allied Command Transformation under the 2012 Cyber Defence Programme of Work. This document is a working paper that may not be cited as representing formally approved NCIA, ACT or NATO opinions, conclusions or recommendations, and represents the views of only the authors.

Introduction

- ***Cyber-Defence Data Exchange and Collaboration Infrastructure***
  - ***Facilitate information sharing.***
  - ***Enable automation.***
  - ***Facilitate the generation, refinement and vetting of data through burden-sharing collaboration or outsourcing.***

Work on what you know best, and connect to the best of the rest

Introduction

- ***11 High level Requirements***
  - Comprehensive and sufficient list of CSIRT Knowledge Management requirements
- ***Validation***
- ***Discussion***

Work on what you know best, and connect to the best of the rest

CDXI High-Level Requirements

Provide an adaptable, scalable, secure and decentralized infrastructure based on a freely available core

Work on what you know best, and connect to the best of the rest

CDXI High-Level Requirements

Provide for the controlled evolution of the syntax and semantics of multiple independent data models and their correlation

Work on what you know best, and connect to the best of the rest

CDXI High-Level Requirements

Securely store both shared and private data

Work on what you know best, and connect to the best of the rest

CDXI High-Level Requirements

Provide for customizable, controlled multilateral sharing

Work on what you know best, and connect to the best of the rest

CDXI High-Level Requirements

Enable the exchange of data across non-connected domains

Work on what you know best, and connect to the best of the rest

CDXI High-Level Requirements

Provide human and machine interfaces

Work on what you know best, and connect to the best of the rest

CDXI High-Level Requirements

Provide collaborative tools that enable burden sharing for the generation, refinement, and vetting of data

Work on what you know best, and connect to the best of the rest

CDXI High-Level Requirements

Provide customizable quality-control processes

Work on what you know best, and connect to the best of the rest

CDXI High-Level Requirements

Expose dissension to reach consensus

Work on what you know best, and connect to the best of the rest

CDXI High-Level Requirements

Support continuous availability of data

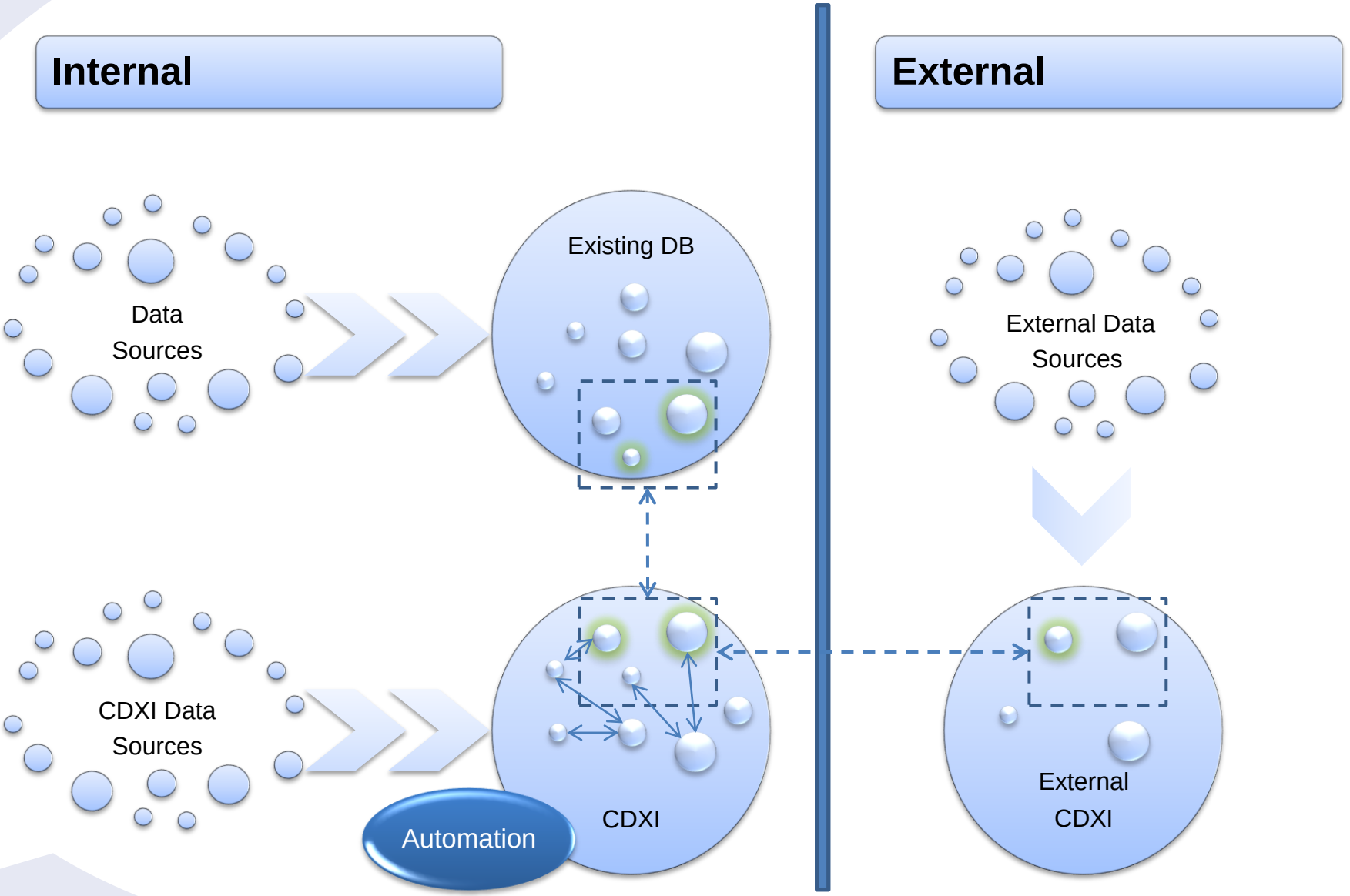
Work on what you know best, and connect to the best of the rest

CDXI High-Level Requirements

Enable commercial activities

Work on what you know best, and connect to the best of the rest

Integration with Other Data Sources



Way Forward

- Feedback
- Validation of the capability

Questionnaire!

For those interested

- Leave me your contact information
- I can provide a copy of the capability definition
- Paper will be published at the CyCon 2013 conference

- Preparation of a workshop

Questions?

- Can it be done?
  - Yes, it is complex but think about no-SQL, multi-versioned data Bases, P2P Data Bases, research on Collaborative Data Sharing Systems.
- It is going to be expensive/complex?
  - Yes, but it is cheap compared to the cost of what is being done now (manual and semi-manual data management with limited effectiveness) and the cost of not doing anything (missed opportunities).
- It would be simpler to …?
  - You did not get it… we are not towards something simple, but towards something comprehensive and future-proof.

Back-up

Background

- There are no mechanisms available to automate large-scale information sharing.
- Many different sources of data containing inconsistent and in some cases erroneous data exist.
- It is difficult, in some cases, to access the desired information from the large volumes of data stored on the Internet or embedded in specific products (e.g. vulnerability repositories, signatures for anti-virus products, etc.).
- Many protocols and access mechanisms are proprietary or not interoperable.
- Incompatible semantics using the same or similar words are used in different data sources covering the same topics.
- The quality of data varies and information and assurance regarding the level of quality provided is lacking.
- There is very limited support for efficient collaboration, despite the availability of subject-matter experts in a large number of organizations willing to collaborate.
- Concerns regarding the confidentiality of exchanged data in the absence of means by which redistribution can be satisfactorily controlled must be addressed.