Objectives of the CDXI

- Improve Cyber Defence activities such as
  - Patching Systems
  - Vulnerability Analysis
  - Intrusion Detection
  - Forensics
  - Red Teaming

- Enable automated response
  - Blocking ports, IP addresses
  - Shutting down vulnerable services
  - Quarantining compromised hosts/networks

- Distribute the workload of maintaining Cyber Defence
  “Reference Data”
CDXI Reference Data

- Data on the following key topics common to all Cyber Defence activities:
  - Software (Operating systems and applications)
  - Hardware
  - Vulnerabilities
  - Malware
  - Fixes
  - Verification Tests (e.g. IDS signatures and VA tests)
  - Protocols

- Nothing that is specific to an organization (no IP addresses, no incident data, etc.)
The CDXI can be seen as a service providing *Reference Data* to security products and custom applications.

Reference Data consists of:

- Pure enumerations on key topics common to all Cyber Defence activities
- Relationships between elements in these topics
- Supporting information and meta-data

For these objectives, the CDXI will provide an API through which *Reference Data* can be integrated into security products and custom applications.
Distributing the Workload

- The CDXI must provide:
  - a user interface to manage the data
  - collaboration tools to discuss problems with the data
  - version control of records so that "many truths can coexist until the ultimate truth is found"

- The CDXI must make it easier for people to contribute Reference Data back to the community

- The CDXI must enable data mining by allowing users to develop custom classification schemes and relationships
Automating Cyber Defence

- Accuracy and integrity of the Reference Data is critical
- To ascertain the accuracy of Reference Data:
  - The CDXI must provide the mechanism to develop and use custom “Quality Assurance” processes
- To ensure integrity:
  - The CDXI must allow for the cryptographic signing of Reference Data and QA records
Other Required Features

- Granular access controls to allow for private data and controlled sharing within communities of interest
- Encryption of data to allow for commercial exploitation
  - Feeds of reference data can be sold
  - Quality assurance can be sold
  - Data-mining can be outsourced
CDXI Schematic

Operational Data

- VA App
- ID App
- Red Team App
- Company Specific DB

Reference Data

- CDXI Local Node
- CDXI Exchange Node
- CDXI Master Node
- API
- CDXI User Interface

“Control Barrier”
- Only QA’ed data is brought in
- No Operational data goes out
CDXI Status

- Concept has been in development for a number of years, including some prototyping
- Detailed NATO requirements and specifications to be completed in 2010
- Initial prototype planned for development in 2011
- Currently seeking to establish contact with interested parties to:
  - Share our results where possible
  - Obtain additional input from various communities
  - Perhaps collaborate on the prototype?
Conclusion

- The CDXI will be a service that provides Reference Data directly into security applications
- The CDXI will be sort of a Wikipedia of Reference data, but with the addition of:
  - Structure to enable machine processing
  - Trust to enable automation
  - Access Controls to control sharing
  - Support for Commercial Exploitation

For additional information, please contact:

luc.dandurand@nc3a.nato.int