



I N S P I R E

EC Grant Agreement n. 225553

INSPIRE: INcreasing Security and Protection through Infrastructure REsilience

The OSF Vulnerability Collector

Component Presentation Video

Elyoenai Egozcue
S21sec
eegozcue@s21sec.com



Outline



EC Grant Agreement n. 225553

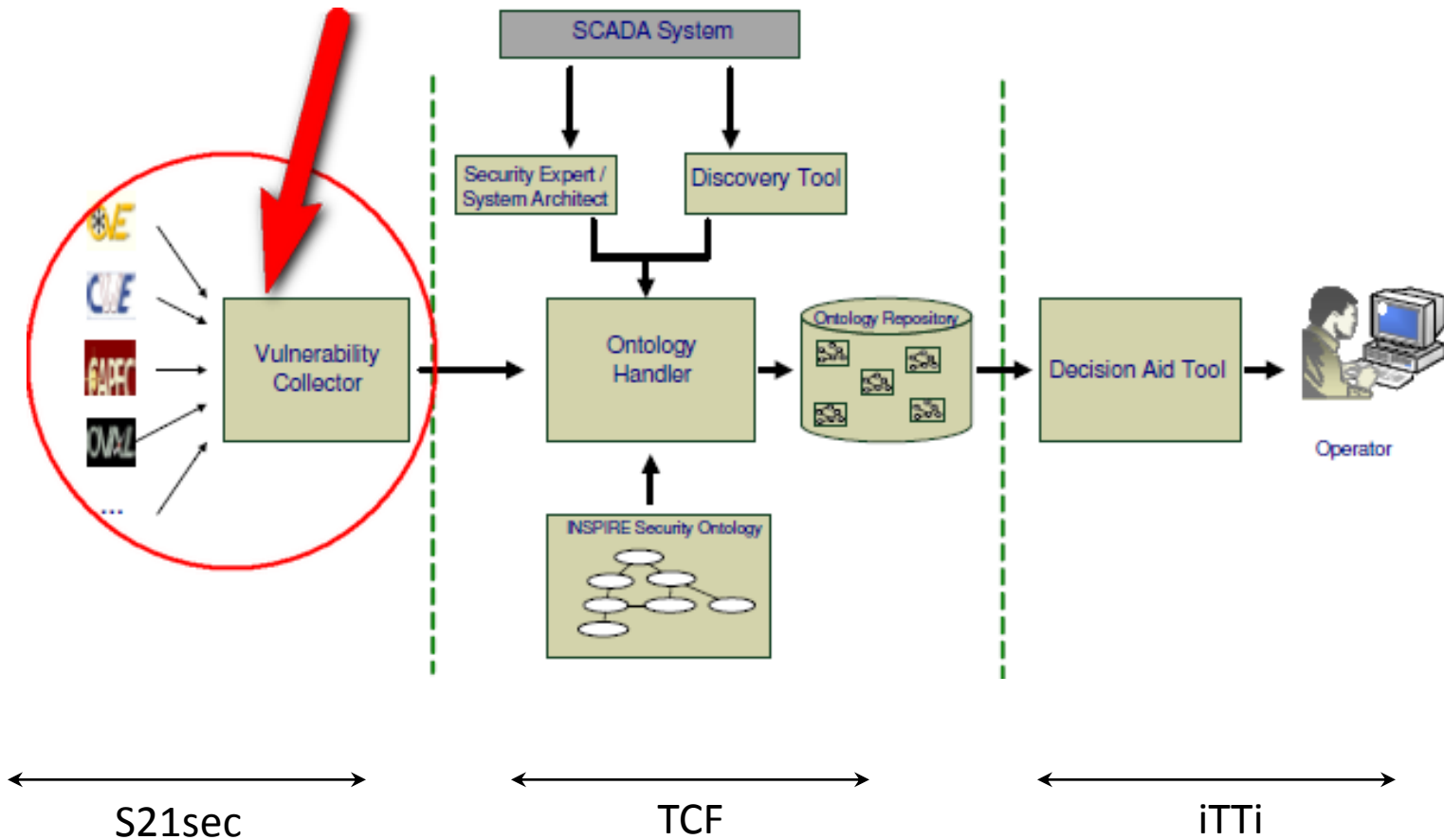
I N S P I R E

- Where does the VC fit inside the OSF?
- Key objectives of the VC
- Information sources
- The indexing process
- VC's logical components
- VC's features overview
- VC's interfaces: app-to-app and maintenance

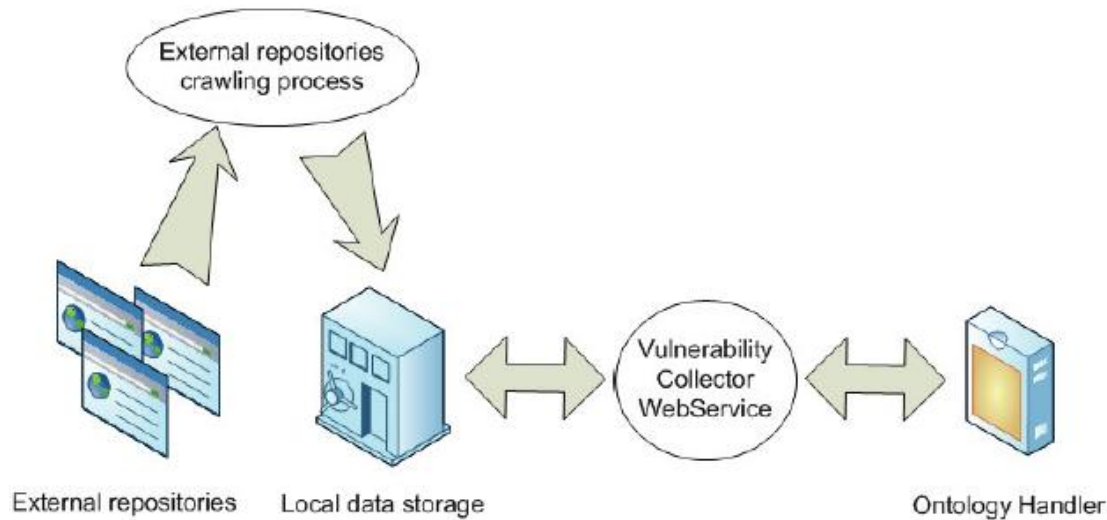
Where the VC fits

I N S P I R E

EC Grant Agreement n. 225553

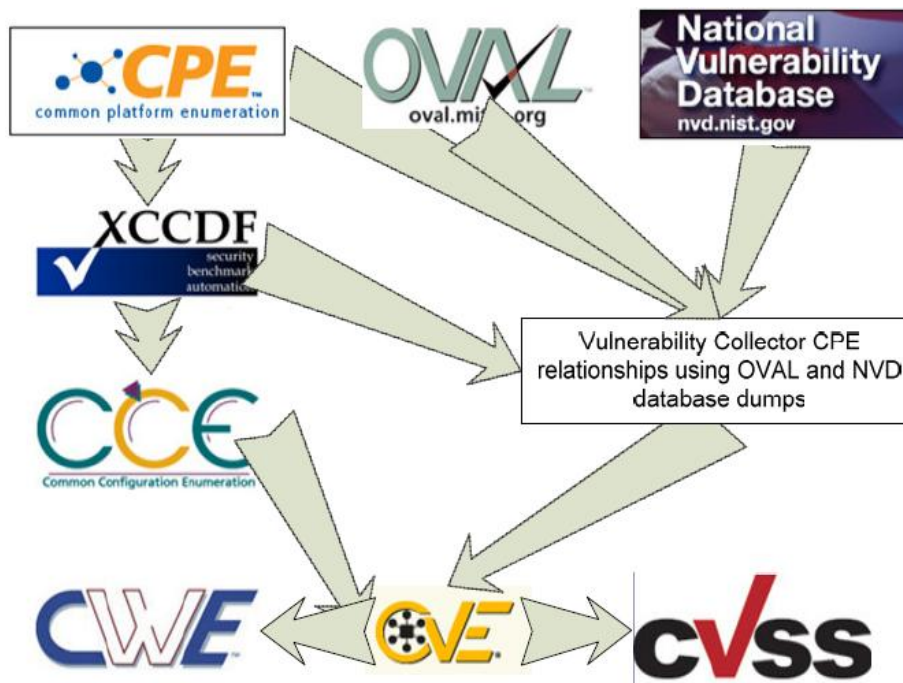


Main Goal: Automatically aggregate **vulnerabilities, weaknesses, threats, and safeguards** from different **external sources** and consolidate this info in a **single centralized place**



Key Objectives

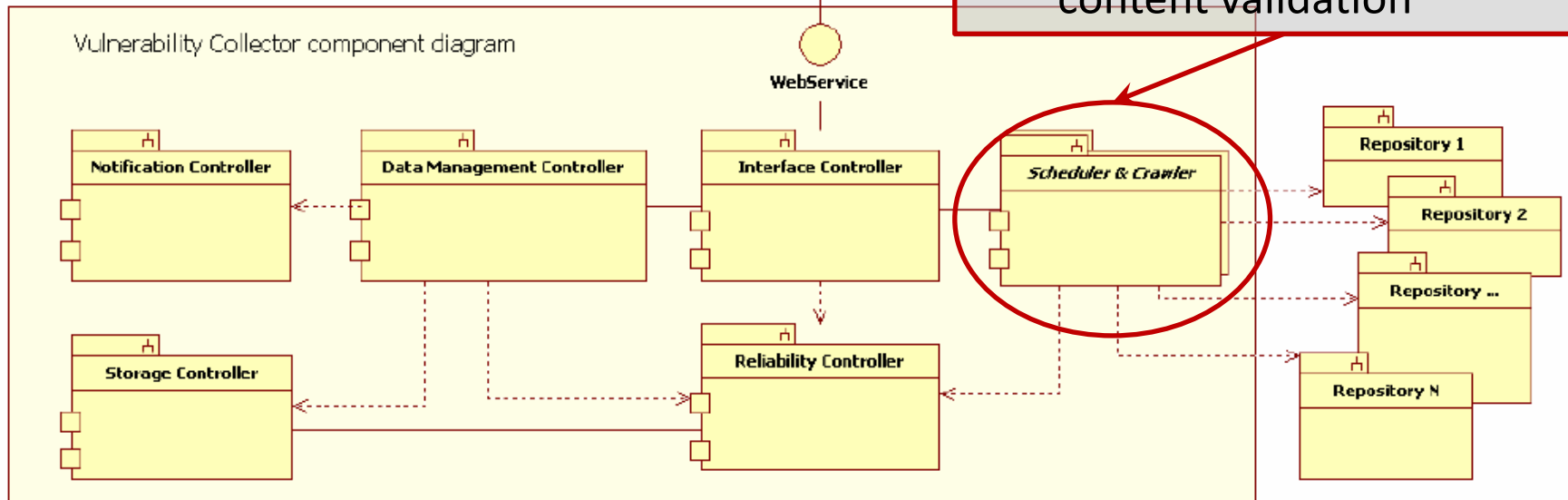
- Maintain a constantly **updated information** storage
- Keep information **uniqueness**
- **Index and relate** the information coming from different sources

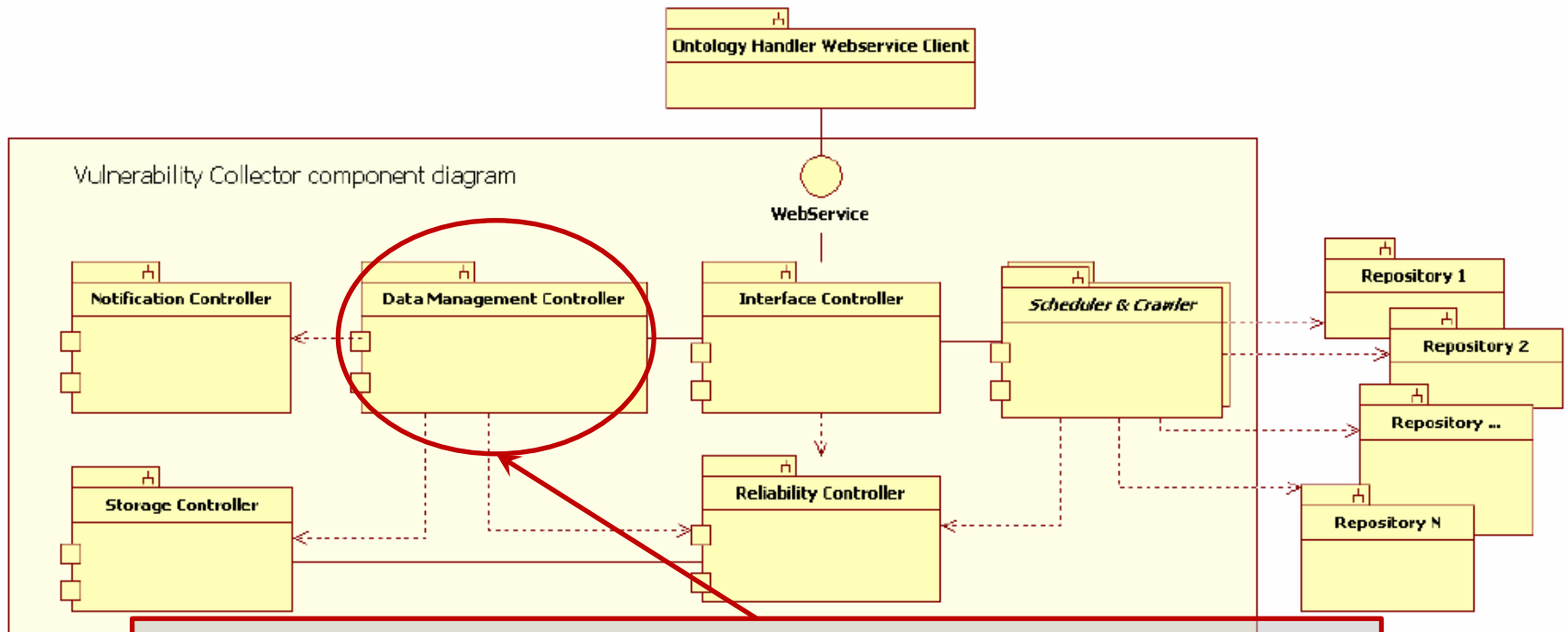


Pivot Points

- **Def:** A unique identifier for any data entry of any of these repositories
- Pivot points can be used as the main input parameter in requests coming from the OH

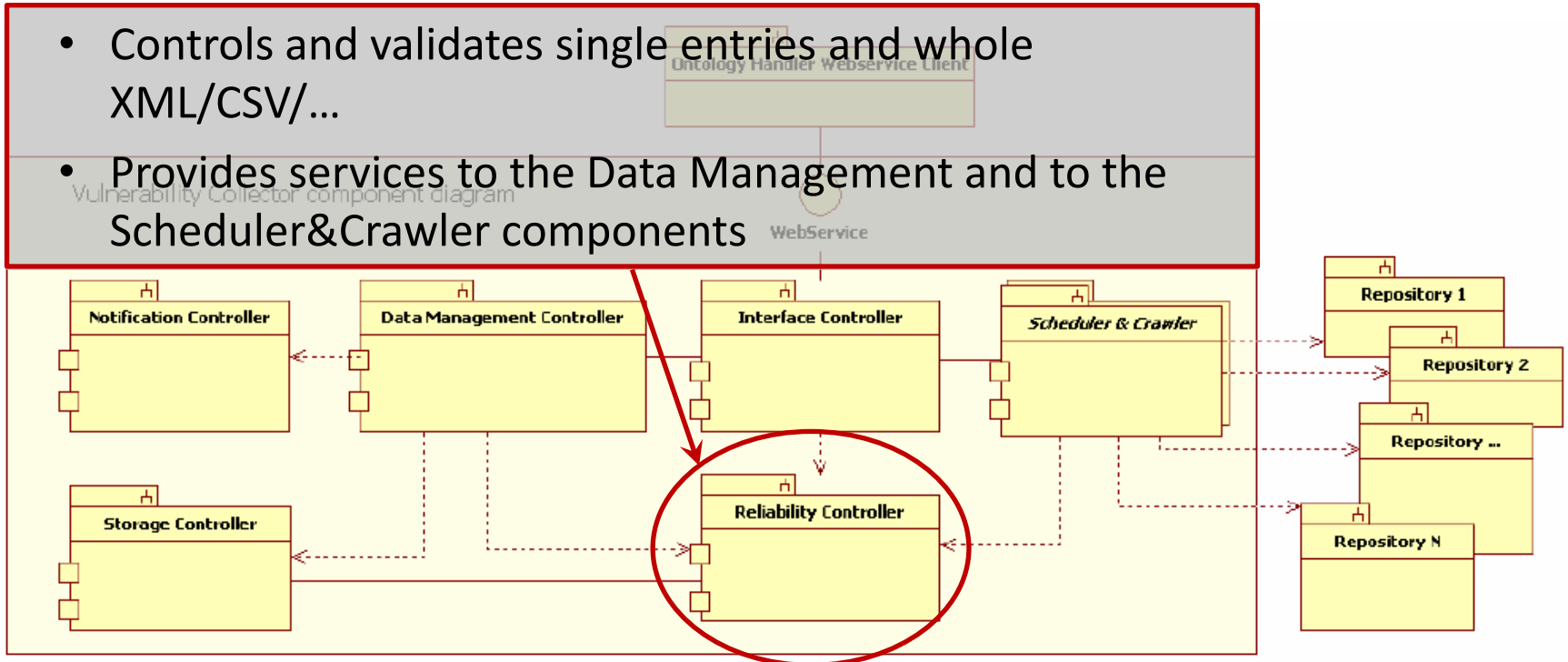
- Checks selected sources periodically
- Fetches and requests content validation

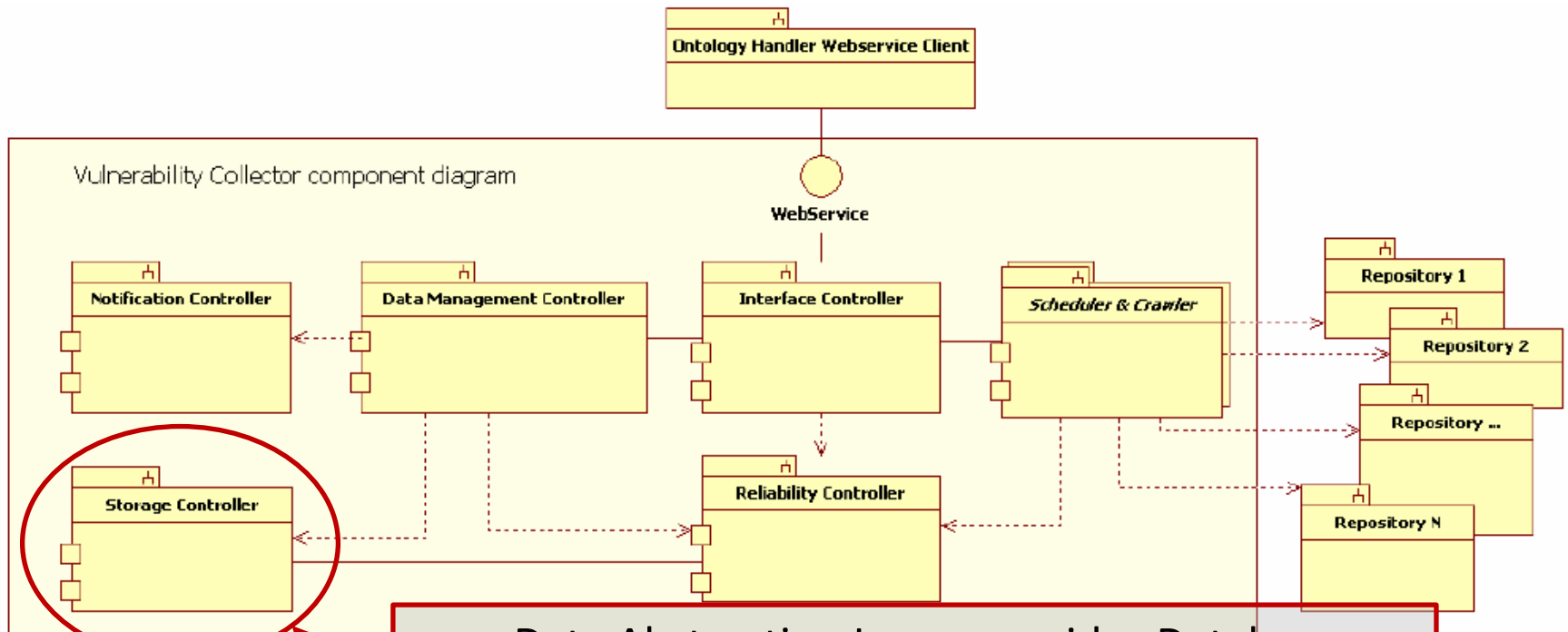




- Processes the info coming from the Scheduler&Crawler and sends it to the Storage Controller
- Responsible for indexing, and requesting entry validation and storage

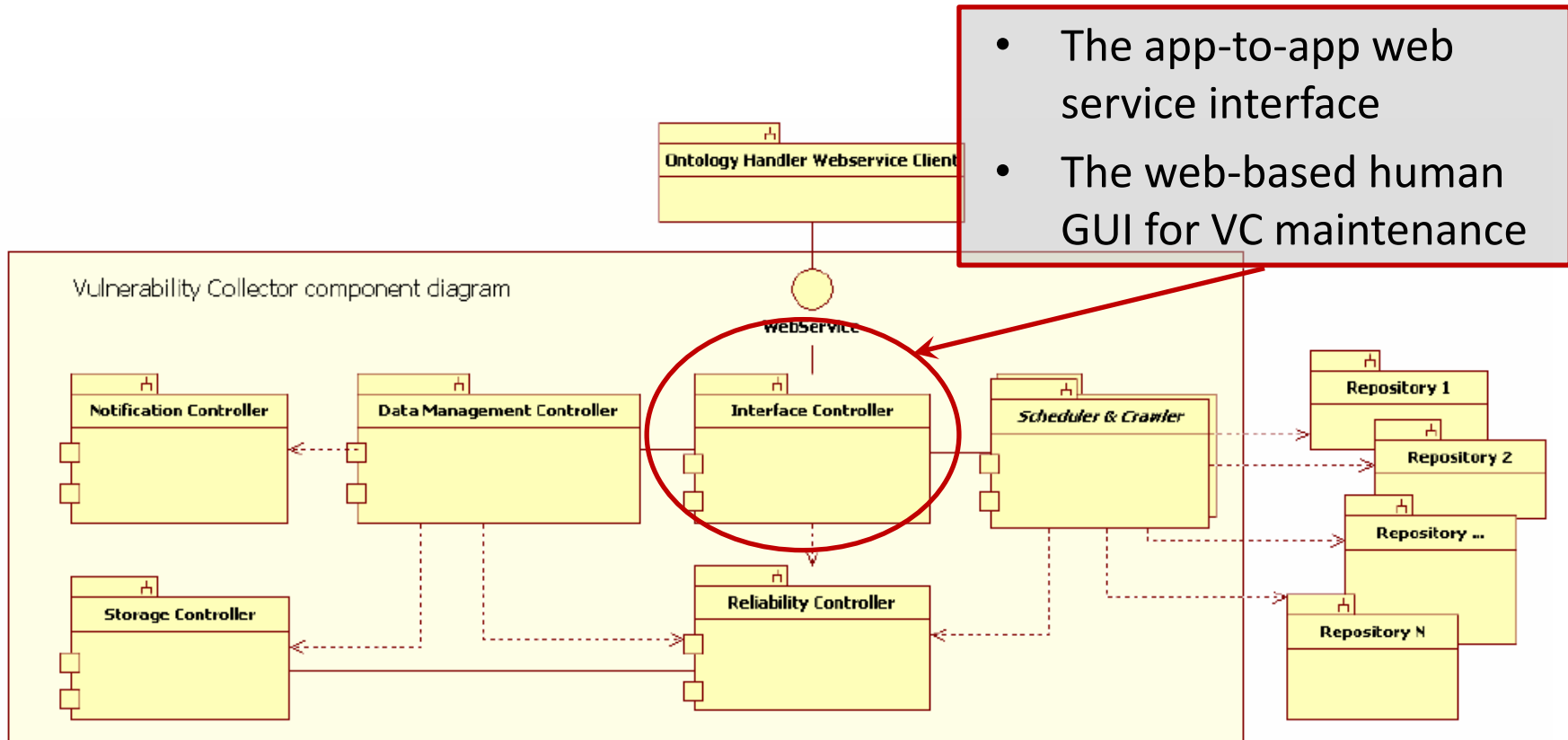
- Controls and validates single entries and whole XML/CSV/...
- Provides services to the Data Management and to the Scheduler&Crawler components

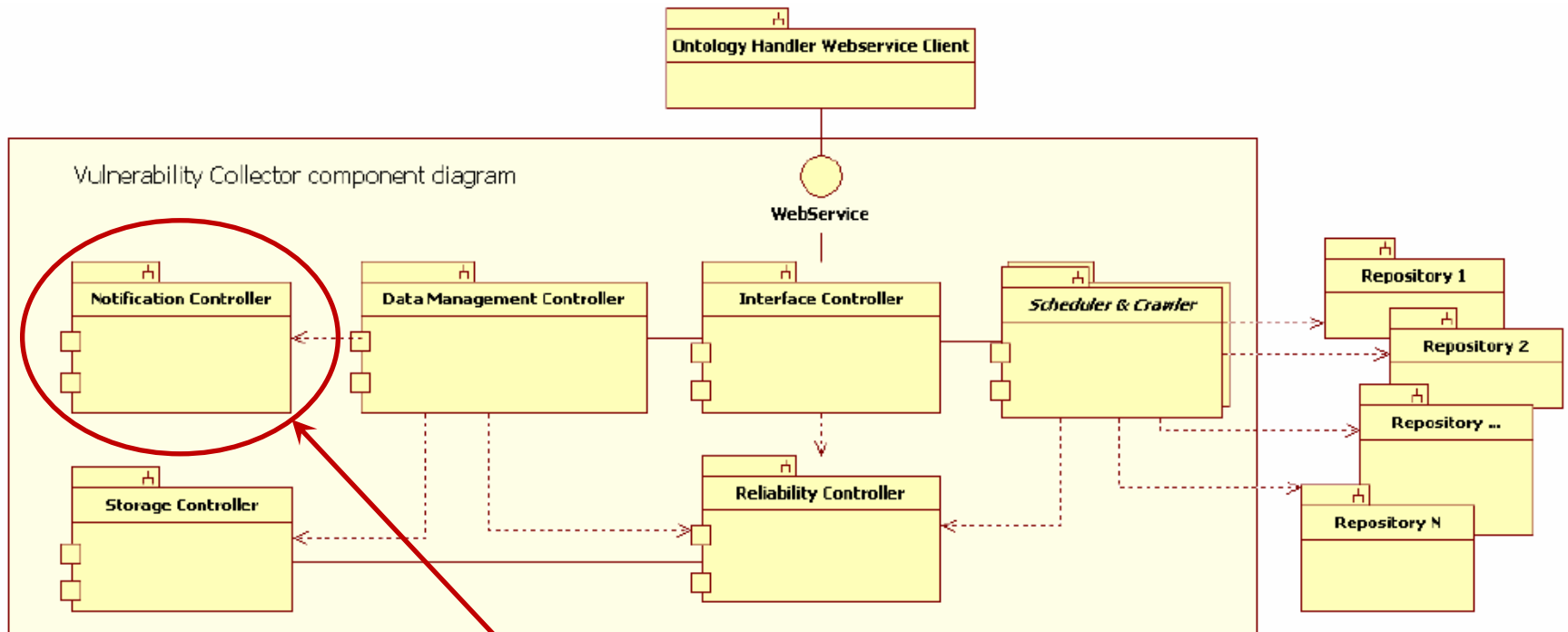




- Data Abstraction Layer, provides Database engine and/or file system independency.
- Stores security information (CVE, CPE, CAPEC, CWE, ...) in a relational database.

- The app-to-app web service interface
- The web-based human GUI for VC maintenance





- Alerts the VC maintainer about consolidation requirements or other issues
- eMail and RSS feeds



Features. Overview



I N S P I R E

EC Grant Agreement n. 225553

- **Feeds or bulk dumps** from **several locations** (currently only official repos.)
- Through **HTTP** or/and **Local Storage**
- **Automatically** grabbed (crawler and scheduler)
- Stored on their **original format** (preferably XML)
- **Handling of data duplicates** (namespaces by source: Mitre, Bugtraq, INSPIRE, etc.)
- **Data validation**: automated validation of XML files and their entries (uniqueness, Schema compliance, etc.)
- Manual **disambiguation** through a **web-based maintenance** interface
- **Relational database** for storing security information (CVE, CPE, CWE, OVAL, CCE and CAPEC)
- **Data Abstraction Layer** for DB engine and/or file-system independency

- **Web** interface
- **User management:** addition/removal
- **Authentication** and role-based authorization
- **Crawling** and **scheduling** processes configuration
- Direct **data management:** create, modify and delete database entries.
- **Manual Consolidation** and disambiguation
- **Database backup** and restoring activities (scheduled & manual)
- **Alert notification** configuration: eMail, RSS and web



inspirevc.s21sec.com/vc/admin/user

Content management Site building Site configuration User management Reports Help

inspirevc.s21sec.com

Home > Administer

admin

- Code review
- My account
- ▶ Create content
- ▼ Administer
 - ▶ Content management
 - ▶ Site building
 - ▶ Site configuration
 - ▼ User management
 - Access rules
 - Permissions
 - Roles
 - User settings
 - Users
 - ▶ Reports
 - Help

User management

- Access rules
List and create rules to dis
- Permissions
Determine access to featu
- Roles
List, edit, or add user roles
- User settings
Configure default behavior
- Users
List, add, and edit users.

- **Super admin:** manage the server and the application
- **Operator:** manage the VC contents, the feeds, execute the internal tests and manage disambiguations
- **Security expert:** verify the VC status, updates the feeds and use the VC
- **Users:** any user with the capacity to get the information through the web service

- **SOAP**, RESTFUL and HTTP GET protocols
- WSDL-based API, agreed with TCF to query for Pivot Points.
`retrieveVulnerabilities('cpe:/o:microsoft:windows_server_2003')`
- The output is an **XML-formatted** dump
- It is an **ordered set** of the **original (raw)** XML/CVS/... entries (validation against their sources)
- Which are related to the particular pivot point requested (i.e. CPEid)
- **What does ordered stand for?** Elements directly related through the pivot point will come first, then those with a two-hop distance, etc.

```

<?xml version="1.0" ?>
<catalog>
  <source_type>
    <id></id>
    <namespace></from>
    <source></source>
    <raw></raw>
  </source_type>
  ...
</catalog>

```

