SCAP Content Repository - Preview

Chandrashekhar B

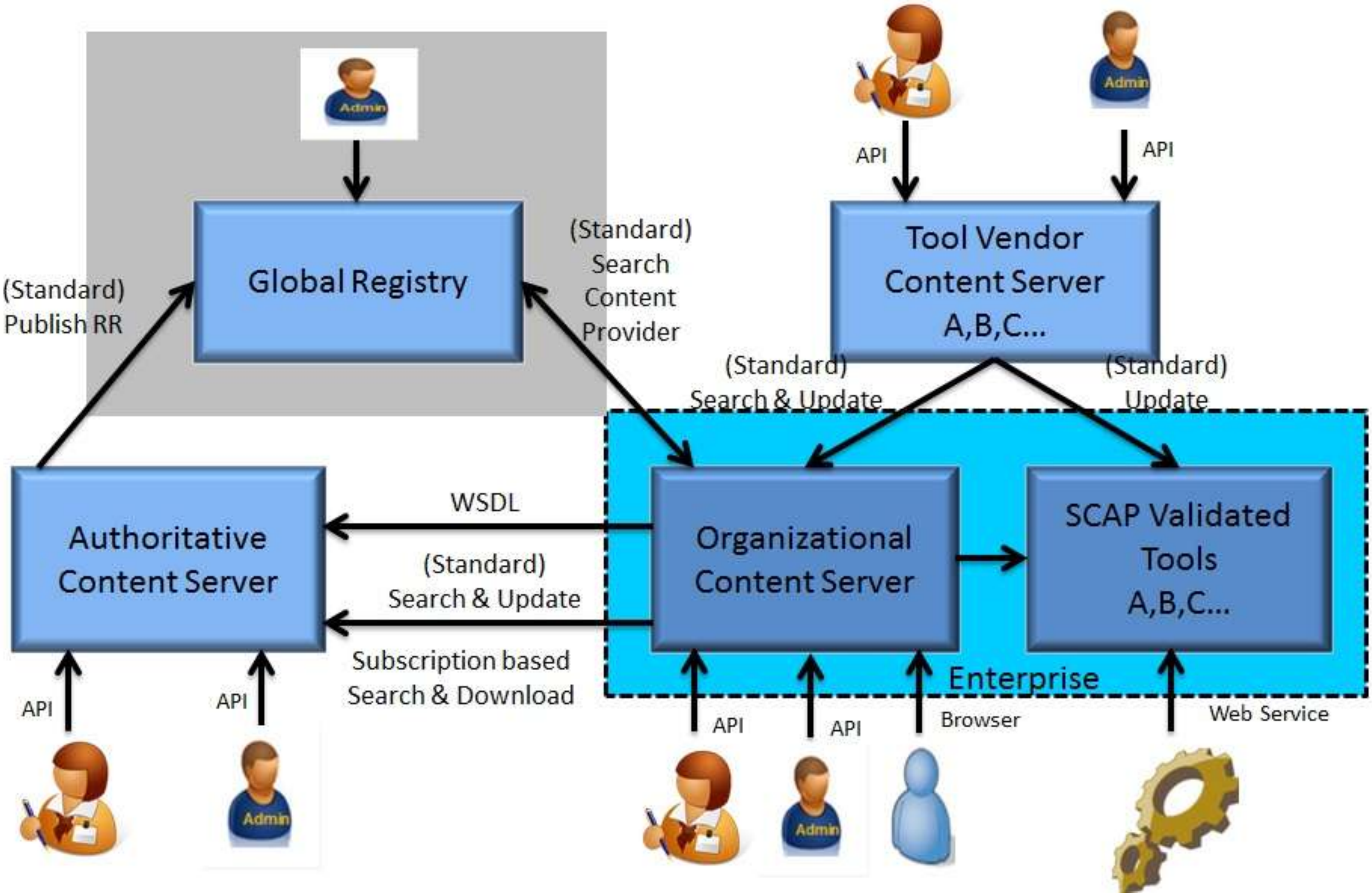
The need

- Standardized security content in a single store
  (Many standards today CVE, CPE, CCE, CVSS, **CCSS**, XCCDF, OVAL, **OCIL**, **AI**, **ARF**)

- Content aggregation from distributed repositories
  - NIST Repository
  - MITRE OVAL Repository
  - OS Vendor Repositories
  - Product Vendors Content (Supported)
  - SecPod Repository (Supported)

- Content Management
  - Global and Local Search for appropriate content
  - Import content
  - Content distribution across SCAP products within the organization
  - Author/Customize content per organizational need

- SC**A**P – all in an automated fashion



Global Registry

(Standard) Publish RR

(Standard) Search Content Provider

Tool Vendor Content Server A,B,C...

API

API

(Standard) Search & Update

(Standard) Update

Authoritative Content Server

WSDL

(Standard) Search & Update

Subscription based Search & Download

Organizational Content Server

SCAP Validated Tools A,B,C...

Enterprise

API

API

API

API

Browser

Web Service

Deployment Scenarios

- Organizational Content Server
- Authoritative Repository Server
- SCAP Product Vendor

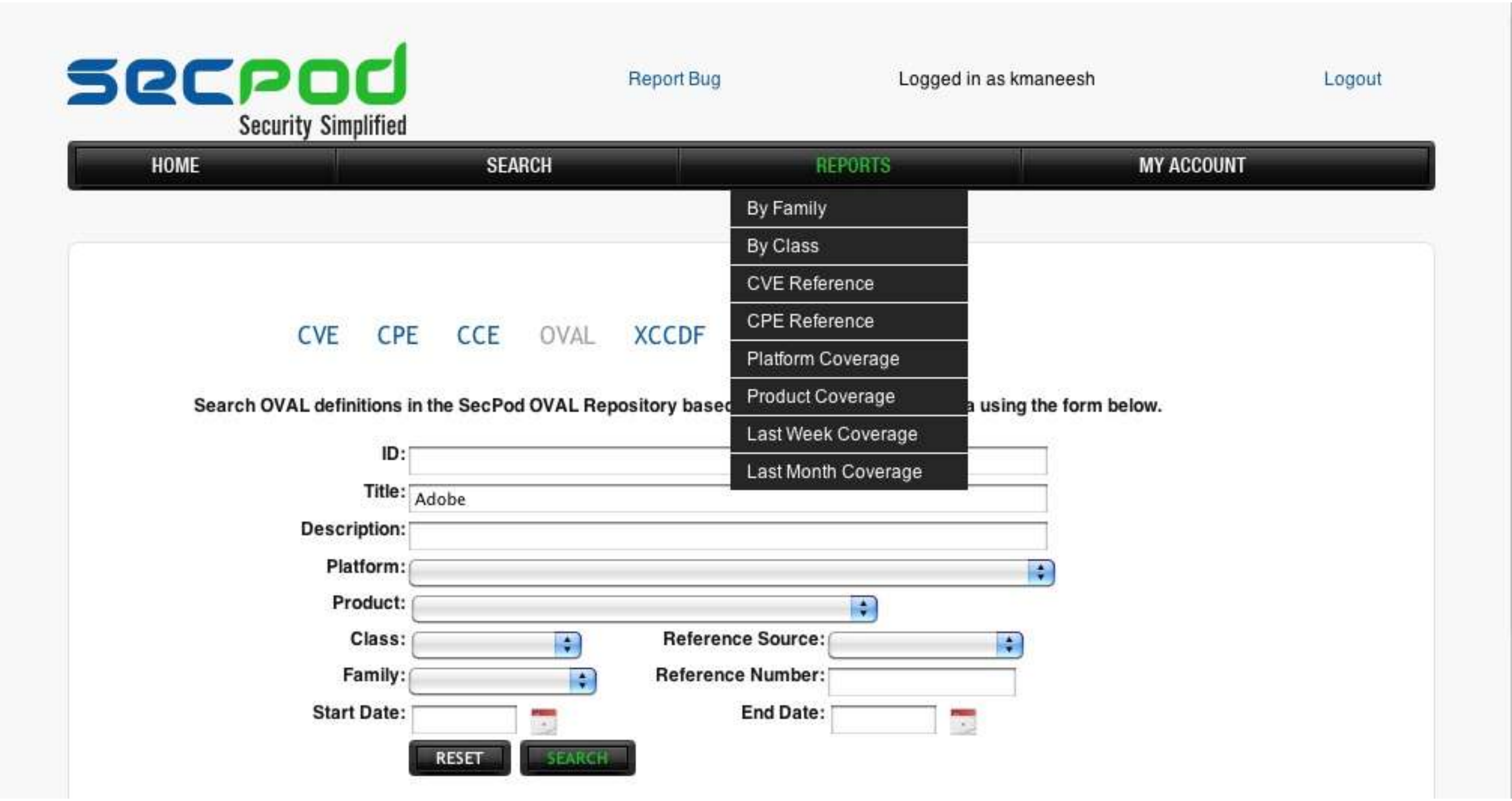
Roles and Use Cases

- Organizational Users
- Organizational Repository Administrator
- A Consumer Program/Product
- Content Authoring/Tailoring

Organizational users

- Search for appropriate content
- Fetch specific content
- Run Risk reports

Organizational users



Logged in as kmaneesh

Search OVAL definitions in the SecPod OVAL Repository based a using the form below.

ID:

Title: Adobe

Description:

Platform:

Product:

Class:

Reference Source:

Family:

Reference Number:

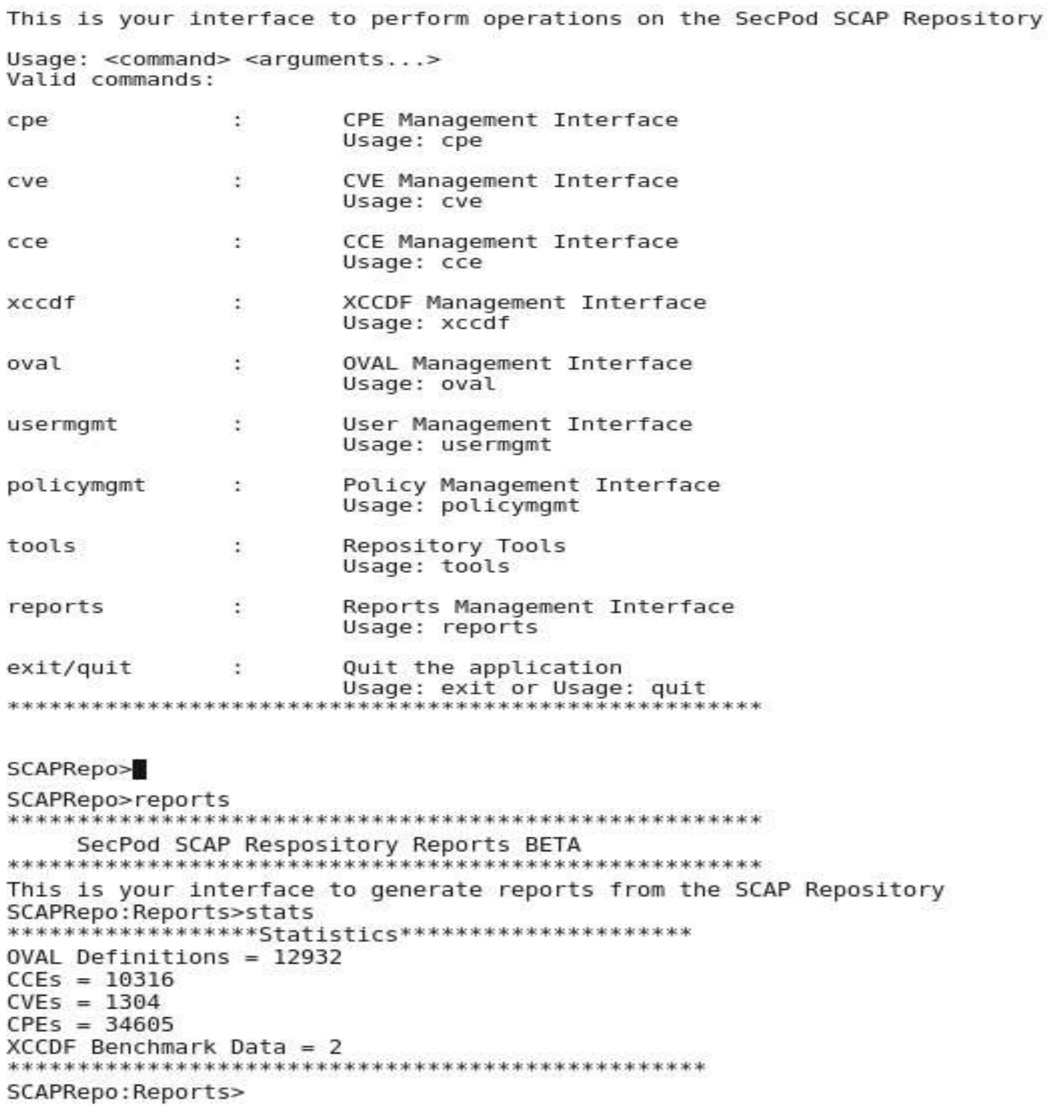
Start Date:

End Date:

Organizational Repository Administrator

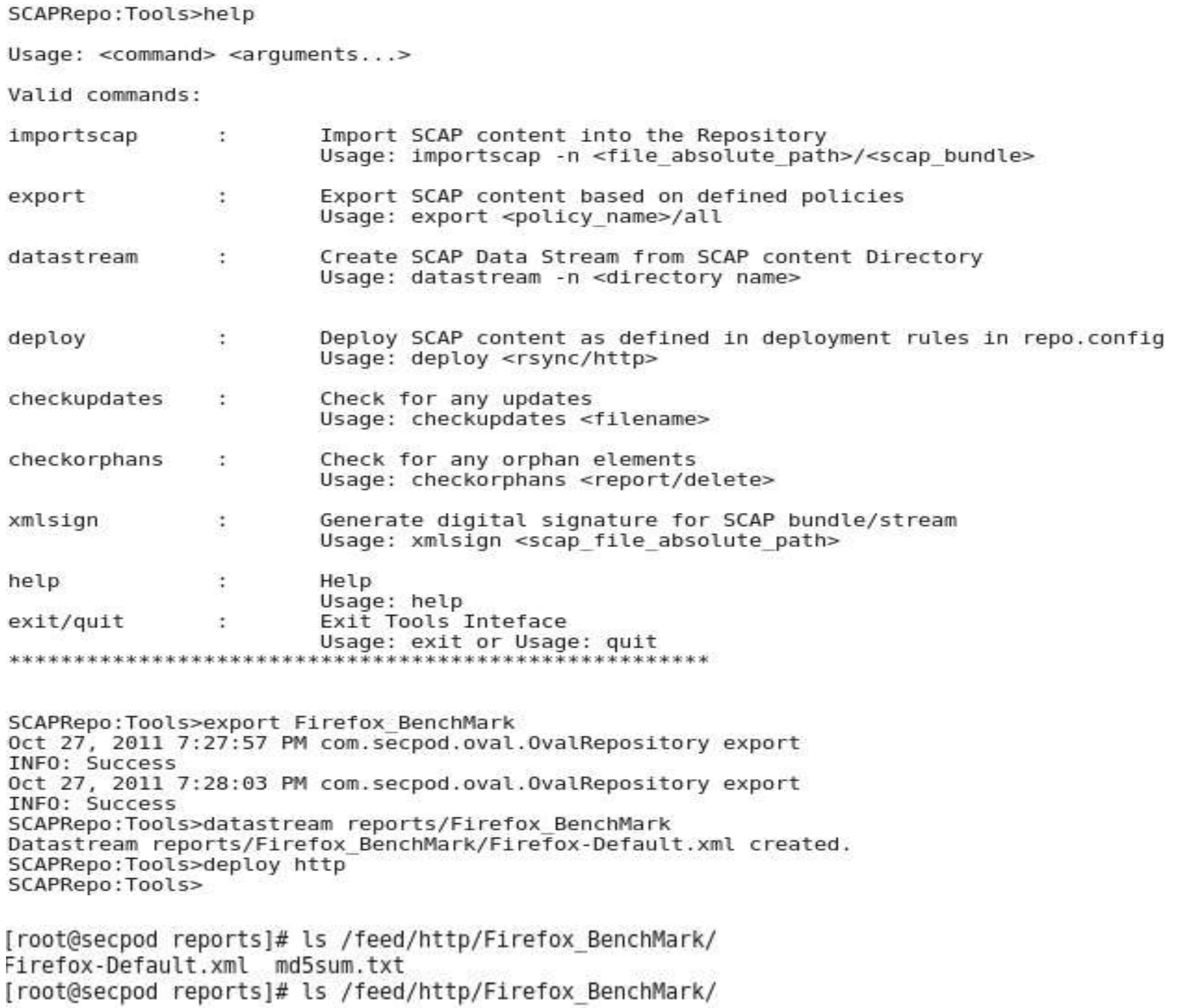
- Global and Local Search for appropriate content
- Import content
- Export the content based on policy and create datastream
- Deploy to a Web, FTP container or Rsync server
- Generate Risk Metrics and alerts
- Maintain repository sanity
- Manage organizational users and policies

Organizational Repository Administrator



```
This is your interface to perform operations on the SecPod SCAP Repository

Usage: <command> <arguments...>
Valid commands:

cpe             :       CPE Management Interface
                        Usage: cpe

cve             :       CVE Management Interface
                        Usage: cve

cce             :       CCE Management Interface
                        Usage: cce

xccdf           :       XCCDF Management Interface
                        Usage: xccdf

oval            :       OVAL Management Interface
                        Usage: oval

usermgmt        :       User Management Interface
                        Usage: usermgmt

policymgmt      :       Policy Management Interface
                        Usage: policymgmt

tools           :       Repository Tools
                        Usage: tools

reports         :       Reports Management Interface
                        Usage: reports

exit/quit       :       Quit the application
                        Usage: exit or Usage: quit
******************************************************


SCAPRepo>
SCAPRepo>reports
******************************************************
     SecPod SCAP Respository Reports BETA
******************************************************
This is your interface to generate reports from the SCAP Repository
SCAPRepo:Reports>stats
******************Statistics*********************
OVAL Definitions = 12932
CCEs = 10316
CVEs = 1304
CPEs = 34605
XCCDF Benchmark Data = 2
**************************************************
SCAPRepo:Reports>
```

Organizational Repository Administrator

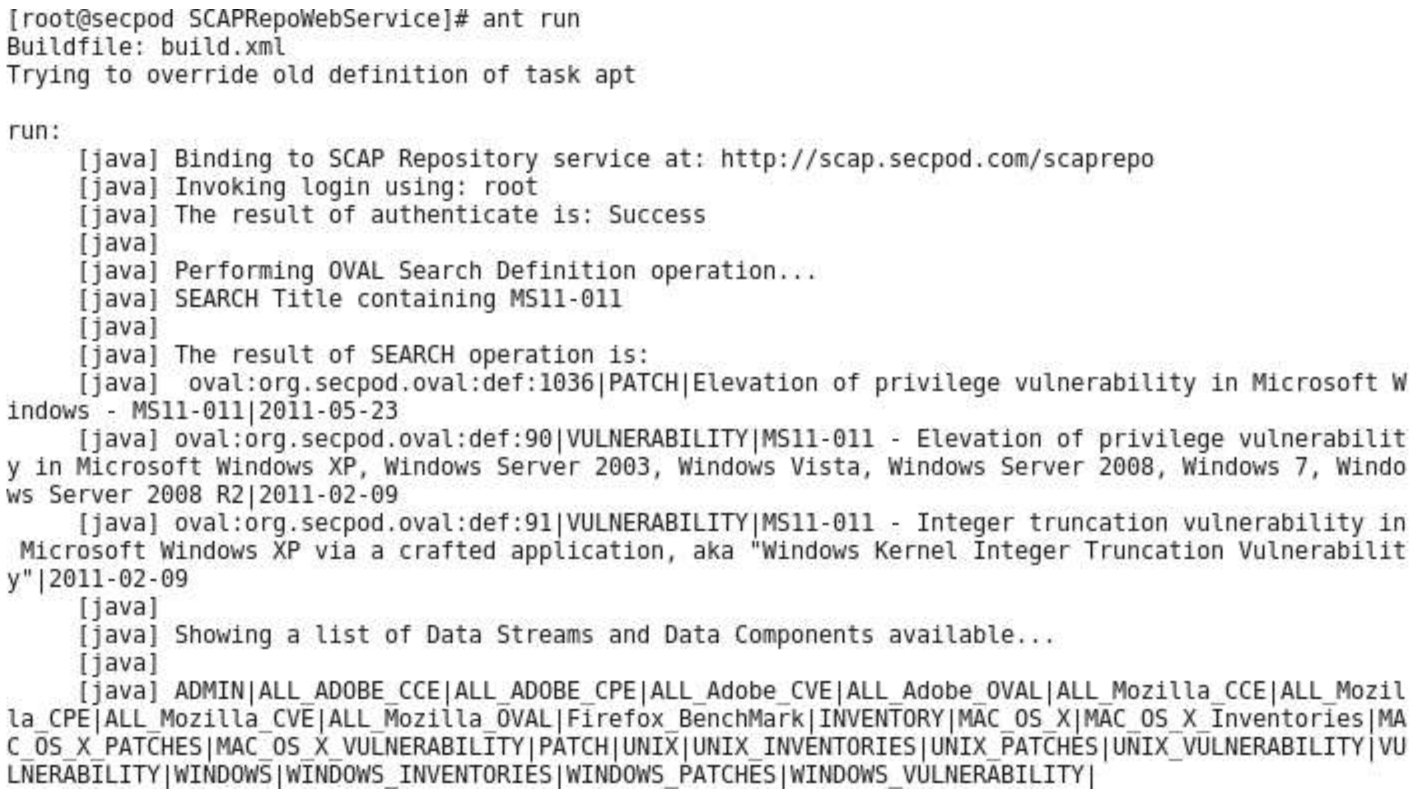


```
SCAPRepo:Tools>help

Usage: <command> <arguments...>

Valid commands:

importscap      :       Import SCAP content into the Repository
                        Usage: importscap -n <file_absolute_path>/<scap_bundle>

export          :       Export SCAP content based on defined policies
                        Usage: export <policy_name>/all

datastream      :       Create SCAP Data Stream from SCAP content Directory
                        Usage: datastream -n <directory name>


deploy          :       Deploy SCAP content as defined in deployment rules in repo.config
                        Usage: deploy <rsync/http>

checkupdates    :       Check for any updates
                        Usage: checkupdates <filename>

checkorphans    :       Check for any orphan elements
                        Usage: checkorphans <report/delete>

xmlsign         :       Generate digital signature for SCAP bundle/stream
                        Usage: xmlsign <scap_file_absolute_path>

help            :       Help
                        Usage: help
exit/quit       :       Exit Tools Inteface
                        Usage: exit or Usage: quit
******************************************************


SCAPRepo:Tools>export Firefox_BenchMark
Oct 27, 2011 7:27:57 PM com.secpod.oval.OvalRepository export
INFO: Success
Oct 27, 2011 7:28:03 PM com.secpod.oval.OvalRepository export
INFO: Success
SCAPRepo:Tools>datastream reports/Firefox_BenchMark
Datastream reports/Firefox_BenchMark/Firefox-Default.xml created.
SCAPRepo:Tools>deploy http
SCAPRepo:Tools>

[root@secpod reports]# ls /feed/http/Firefox_BenchMark/
Firefox-Default.xml  md5sum.txt
[root@secpod reports]# ls /feed/http/Firefox_BenchMark/
```

A Consumer Program/Product

- Web Services model (WSDL)
- Query what it wants – build programs with ***standardized*** search queries
- Query its entitlements – List all Data Stream or Bundle it can fetch
- Query the Data Stream or Bundle URI, URI can be HTTP, FTP, SCP, Rsync

A Consumer Program/Product



```
[root@secpod SCAPRepoWebService]# ant run
Buildfile: build.xml
Trying to override old definition of task apt

run:
     [java] Binding to SCAP Repository service at: http://scap.secpod.com/scaprepo
     [java] Invoking login using: root
     [java] The result of authenticate is: Success
     [java]
     [java] Performing OVAL Search Definition operation...
     [java] SEARCH Title containing MS11-011
     [java]
     [java] The result of SEARCH operation is:
     [java]  oval:org.secpod.oval:def:1036|PATCH|Elevation of privilege vulnerability in Microsoft W
indows - MS11-011|2011-05-23
     [java] oval:org.secpod.oval:def:90|VULNERABILITY|MS11-011 - Elevation of privilege vulnerabilit
y in Microsoft Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7, Windo
ws Server 2008 R2|2011-02-09
     [java] oval:org.secpod.oval:def:91|VULNERABILITY|MS11-011 - Integer truncation vulnerability in
 Microsoft Windows XP via a crafted application, aka "Windows Kernel Integer Truncation Vulnerabilit
y"|2011-02-09
     [java]
     [java] Showing a list of Data Streams and Data Components available...
     [java]
     [java] ADMIN|ALL_ADOBE_CCE|ALL_ADOBE_CPE|ALL_Adobe_CVE|ALL_Adobe_OVAL|ALL_Mozilla_CCE|ALL_Mozil
la_CPE|ALL_Mozilla_CVE|ALL_Mozilla_OVAL|Firefox_BenchMark|INVENTORY|MAC_OS_X|MAC_OS_X_Inventories|MA
C_OS_X_PATCHES|MAC_OS_X_VULNERABILITY|PATCH|UNIX|UNIX_INVENTORIES|UNIX_PATCHES|UNIX_VULNERABILITY|VU
LNERABILITY|WINDOWS|WINDOWS_INVENTORIES|WINDOWS_PATCHES|WINDOWS_VULNERABILITY|
```

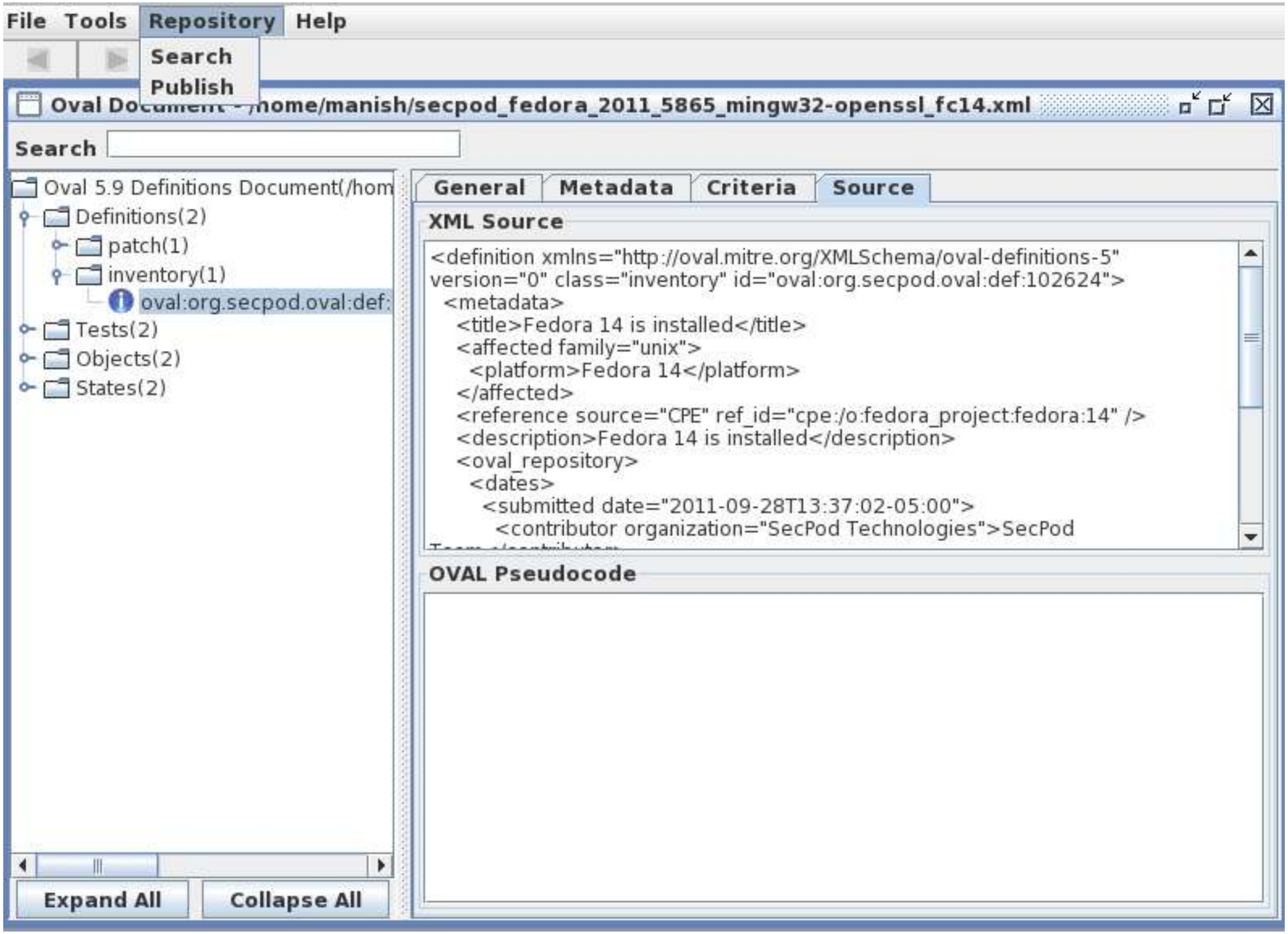
…

…

Content Authoring/Tailoring

- Search for appropriate content
- Reuse content
- Author content
- Publish content

Content Authoring/Tailoring



```
<definition xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5"
version="0" class="inventory" id="oval:org.secpod.oval:def:102624">
  <metadata>
    <title>Fedora 14 is installed</title>
    <affected family="unix">
      <platform>Fedora 14</platform>
    </affected>
    <reference source="CPE" ref_id="cpe:/o:fedora_project:fedora:14" />
    <description>Fedora 14 is installed</description>
    <oval_repository>
      <dates>
        <submitted date="2011-09-28T13:37:02-05:00">
          <contributor organization="SecPod Technologies">SecPod
Team </contributor>
```

How we use at SecPod

- As a Content Repository for a subscription based SCAP Content Professional Feed
- Hosted at http://oval.secpod.com

What next?

- Global Registry
- Standardize SCAP search queries
- WSDL for Content Servers
- Does it fit into Continuous Monitoring framework?
- Productize SCAP Content Server

Questions

bchandra@secpod.com