Compliance Management

Thorsten Scherf

Principal Consultant
Red Hat EMEA

July 2013, SLAC Berlin

redhat

Agenda

- Definition
- System Setup
- Real Life Probleme
- SCAP Framework
- SCAP Security Guide
- SCAP Anatomie
- Grafische Tools
- Ressourcen
- Summary

Compliance Management Definition

- Allgemein:
  - Einhaltung von Gesetzen und Unternehmensrichtlinien
  - Traditionell Aufgabe der Rechtsabteilung
    - Kapitalmarkt (SOX)
- IT-Compliance / IT-Governance
  - Einhaltung von Gesetzen und Unternehmensrichtlinien für IT-Services, Prozesse und Systeme
    - Datenschutz (BDSG)
    - Verfügbarkeit
    - Software-Lizenzen
    - **IT-Sicherheit**

redhat

IT Sicherheit

- Software
  - Software Pakete / Patch Management
- System-Konfiguration
  - Konfigurationsdateien / Revision Management
- System-Layout / Härtung
  - Guidelines / Best-practices
- Sonstiges
  - Einbrüche / Forensik / Anomalien

redhat

System Setup/Konfiguration

- Woher weiß ich, wie ich mein System zu konfigurieren habe?
  - Welche Vorgaben (Gesetze, Unternehmensrichtlinien) müssen eingehalten werden?
  - Guidelines
    - OS- und Applikations-Hersteller/Distributoren
    - STIG, CIS Benchmarks
    - PCI/DSS
- Wenn ich weiß wie mein System zu konfigurieren ist, was dann?
  - Baseline erzeugen
    - Base-OS, Datenbanken, App- und Web-Server, ...

redhat

2 Fragen

- Wie stelle ich sicher, das die Baseline auf alle neu zu installierenden Systeme angewendet wird?

- Wie stelle ich sicher, dass meine Systeme auch später noch der Baseline entsprechen?

redhat

Mögliche Antworten

- Komplett **automatisierte** Installation
  - Keine manuellen Konfigurationsschritte
  - Software Management System
  - Config Management System

  => Spacewalk, Katello, Cobbler, Pulp, Puppet, CFEngine,

- Regelmässige **automatisierte** Scans der Systeme
  - Jedes System wird anhand eines Profils überprüft
  - Bei Abweichungen von der Baseline
    - Baseline wieder herstellen (automatisiert)

  => Nessus, OpenVAS, GSTool

redhat

Real-Life Probleme und deren Lösung

- Installation / Konfiguration / Hardening
  - Klassisch: Jeder verwendet seine eigenen Tools / Scripte um die Security-Baseline für ein System umzusetzen

  => Aqueduct ist ein Community-Projekt und stellt Bash- und Puppet-Skripte zur Verfügung (CIS, STIG, ...)

- Scan der Systeme
  - Klassisch: Abarbeitung von Checklisten (PDF, Word-/Excel-Dokumente!)
  - Automatisierung nur mit custom Scripts

  => SCAP – Framework zur Automatisierung von Systemüberprüfungen auf Basis definierter

redhat

OpenSCAP

- Open-Source SCAP Implementierung
  - SCAP 1.2 compliant (released 01/13)
  - NIST Standards (XCCDF, OVAL, CCE, ...)
  - Überprüft die Konfiguration des Systems
  - Überprüft das System auf Software Patches
- OpenSCAP Framework und Content
  - OpenSCAP Engine und Library
  - Content kommt von 3th party Herstellern
    - STIG / SCAP-Security-Guide Project (SSG)
    - Custom
- Integration in System Management Tools

SCAP-Security-Guide (SSG)

- Security Katalog
- Profile basierend auf Regeln
- Alle Regeln basieren auf dem SCAP Framework
- Jede Regel enthält einen Mechanismus zur Validierung
- Aktuelle Regeln existieren für RHEL und JBoss
- Bestehende Regeln können als Grundlage für eigene Profile

  dienen

redhat

SCAP Anatomie

- XCCDF (XML)
  - Spezifikationssprache für Checklisten
  - Enthält Regeln und Profile
  - Regeln verweisen auf Validierungscode (OVAL/SCE)
  - Regeln können Fixes enthalten
- OVAL (XML)
  - Abstrakte Sprache zum Beschreiben von Systemeigenschaften
  - OVAL-Checks werden über XCCDF Regeln referenziert
- *Script Check Engine (SCE)*
  - Gehört nicht zum SCAP Standard
  - XCCDF referenziert Scripte für Systemchecks

redhat

OVAL

- Low-Level (really!)
- Enthält:
  - Definitionen
  - Tests
  - Objekte
  - Eigenschaften
- OVAL Tests benötigen nicht zwingend XCCDF-Content
- Umfangreiches OVAL-Repository mit Advisory-Meldungen der Hersteller
- Besser geeignet als generische Service-Scans

redhat

OVAL tests

Unix schema
- dnscache
- file
- fileextendedattribute
- gconf
- interface
- password
- process
- process58
- routingtable
- runlevel
- shadow
- sysctl
- uname
- xinetd

Linux schema
- dpkginfo
- iflisteners
- inetlisteningservers
- partition
- rpminfo
- rpmverify
- selinuxboolean
- selinuxsecuritycontext

Independent schema
- family
- filehash
- filehash58
- environmentvariable
- environmentvariable58
- ldap57
- textfilecontent
- textfilecontent54
- xmlfilecontent

OVAL Definition

```
<definition class="compliance" id="oval:ssg:def:588" version="1">
    <metadata>
      <title>Ensure SELinux is Properly Enabled</title>
      <affected family="unix">
        <platform>Red Hat Enterprise Linux 6</platform>
      </affected>
      <description>SELinux should be enabled</description>
    <reference source="ssg" ref_id="selinux_enabled"/></metadata>
    <criteria>
      <criterion comment="/selinux exists" test_ref="oval:ssg:tst:589"/>
    </criteria>
 </definition>
 <linux:partition_test check="all" check_existence="all_exist" id="oval:ssg:tst:589" version="1"
comment="/selinux partition exists">
    <linux:object object_ref="oval:ssg:obj:1880"/>
 </linux:partition_test>
 <linux:partition_object id="oval:ssg:obj:1880" version="1">
    <linux:mount_point>/selinux</linux:mount_point>
 </linux:partition_object>
```

Script Check Engine

```
<Rule id="rule-20" selected="true">
    <title>selinux</title>
    <description>
        <xhtml:pre xmlns:xhtml="">Checks if you have SELinux
enabled</xhtml:pre>
    </description>
    <check system="http://open-scap.org/page/SCE">
        <check-import import-name="stdout" />
        <check-content-ref href="selinux.sh" />
    </check>
</Rule>
```

```
#!/usr/bin/env bash
SELINUX_MODE=`/usr/sbin/getenforce`
if [[ $SELINUX_MODE != "Enforcing" ]]
then
        echo "Selinux is in "$SELINUX_MODE" mode."
        echo "Using Enforing mode is highly recommended. See selinux
manual page for switching to Enforcing mode."
        exit $XCCDF_RESULT_FAIL
fi
exit $XCCDF_RESULT_PASS
```

Guide erstellen und System Scan

- XCCDF XML Guide nach HTML konvertieren

```
# oscap xccdf generate guide \
--profile stig-rhel-server \
/usr/share/xml/scap/ssg/content/ssg-rhel6-xccdf.xml \
>stig-rhel6-server-guide.html
```

- System Scan durchführen

```
# oscap xccdf eval \
--profile stig-rhel-server \
--results results.xml \
--report report.html \
--cpe /usr/share/xml/scap/ssg/content/ssg-rhel6-cpe-dictionary.xml \
/usr/share/xml/scap/ssg/content/ssg-rhel6-xccdf.xml
```

redhat

Scan Ergebnis

Score

system	score	max	%	bar
urn:xccdf:scoring:default	50.73	100.00	**50.73%**	

Results overview

Rule Results Summary

pass	fixed	fail	error	not selected	not checked	not applicable	informational	unknown	total
76	0	91	22	177	26	0	0	3	395

Title	Result
Ensure /tmp Located On Separate Partition	pass
Ensure /var Located On Separate Partition	fail
Ensure /var/log Located On Separate Partition	fail
Ensure /var/log/audit Located On Separate Partition	fail
Ensure /home Located On Separate Partition	pass
Ensure Red Hat GPG Key Installed	pass
Disable Red Hat Network Service (rhnsd)	fail
Ensure Software Patches Installed	notchecked
Ensure gpgcheck Enabled In Main Yum Configuration	pass
Ensure gpgcheck Enabled For All Yum Package Repositories	fail
Install AIDE	pass
Ensure SELinux Not Disabled in /etc/grub.conf	error
Remove Rsh Trust Files	pass
Ensure SELinux State is Enforcing	pass
Configure SELinux Policy	pass
Ensure No Device Files are Unlabeled by SELinux	pass
Restrict Virtual Console Root Logins	error

redhat

Detaillierte Scan Ergebnisse

Result for Ensure /tmp Located On Separate Partition

Result: **pass**

Rule ID: **partition_for_tmp**

Time: **2013-02-20 16:25**

Severity: **low**

The `/tmp` directory is a world-writable directory used for temporary file storage. Ensure that it has its own partition or logical volume at installation time, or migrate it using LVM.

The `/tmp` partition is used as temporary storage by many programs. Placing `/tmp` in its own partition enables the setting of more restrictive mount options, which can help protect programs which use it.

Security identifiers

- CCE-14161-4

redhat

Eigene OVAL Definition...

```
<definitions>
    <definition id="oval:tutorial:def:1" class="compliance" version="1">
        <metadata>
            <title>SELinux Policy Installed</title>
            <description>
               Tests if SELinux targeted Policy Pakage is installed.
            </description>
        </metadata>

        <criteria>
            <criterion test_ref="oval:tutorial:tst:1" comment="Check if selinux-policy-targeted package exists"/>
        </criteria>
    </definition>
</definitions>
```

redhat

... und der passende OVAL Test

```
<tests>
    <linux:rpminfo_test check="all" check_existence="all_exist" id="oval:tutorial:tst:1" version="1" comment="package selinux-policy-targeted is installed">
        <linux:object object_ref="oval:tutorial:obj:1"/>
    </linux:rpminfo_test>
</tests>

<objects>
    <linux:rpminfo_object id="oval:tutorial:obj:1" version="1">
        <linux:name>selinux-policy-targeted</linux:name>
    </linux:rpminfo_object>
</objects>
```

Scan und Ergebnis

```
# oscap oval eval --result report.xml tutorial.oval
# oscap oval generate report --output report.html
```

OVAL Results Generator Information				
Schema Version	Product Name	Product Version	Date	Time
5.10	cpe:/a:open-scap:oscap		2013-05-29	10:20:34

OVAL Definition Generator Information				
Schema Version	Product Name	Product Version	Date	Time
5.10	Tutorial	1.0.0	2013-02-06	13:44:00

System Information		
Host Name	tscherf.csb	
Operating System	Linux	
Operating System Version	#1 SMP Sat Nov 24 14:35:28 EST 2012	
Architecture	x86_64	
Interfaces	**Interface Name**	lo
	IP Address	127.0.0.1
	MAC Address	00:00:00:00:00:00
	Interface Name	eth0
	IP Address	10.34.11.25
	MAC Address	F0:DE:F1:D5:C1:25
	Interface Name	virbr0
	IP Address	192.168.122.1
	MAC Address	52:54:00:F7:4D:E0
	Interface Name	lo
	IP Address	::1
	MAC Address	00:00:00:00:00:00
	Interface Name	eth0
	IP Address	fe80::f2de:f1ff:fed5:c125
	MAC Address	F0:DE:F1:D5:C1:25

OVAL System Characteristics Generator Information				
Schema Version	Product Name	Product Version	Date	Time
5.10	cpe:/a:open-scap:oscap		2013-05-29	10:20:34

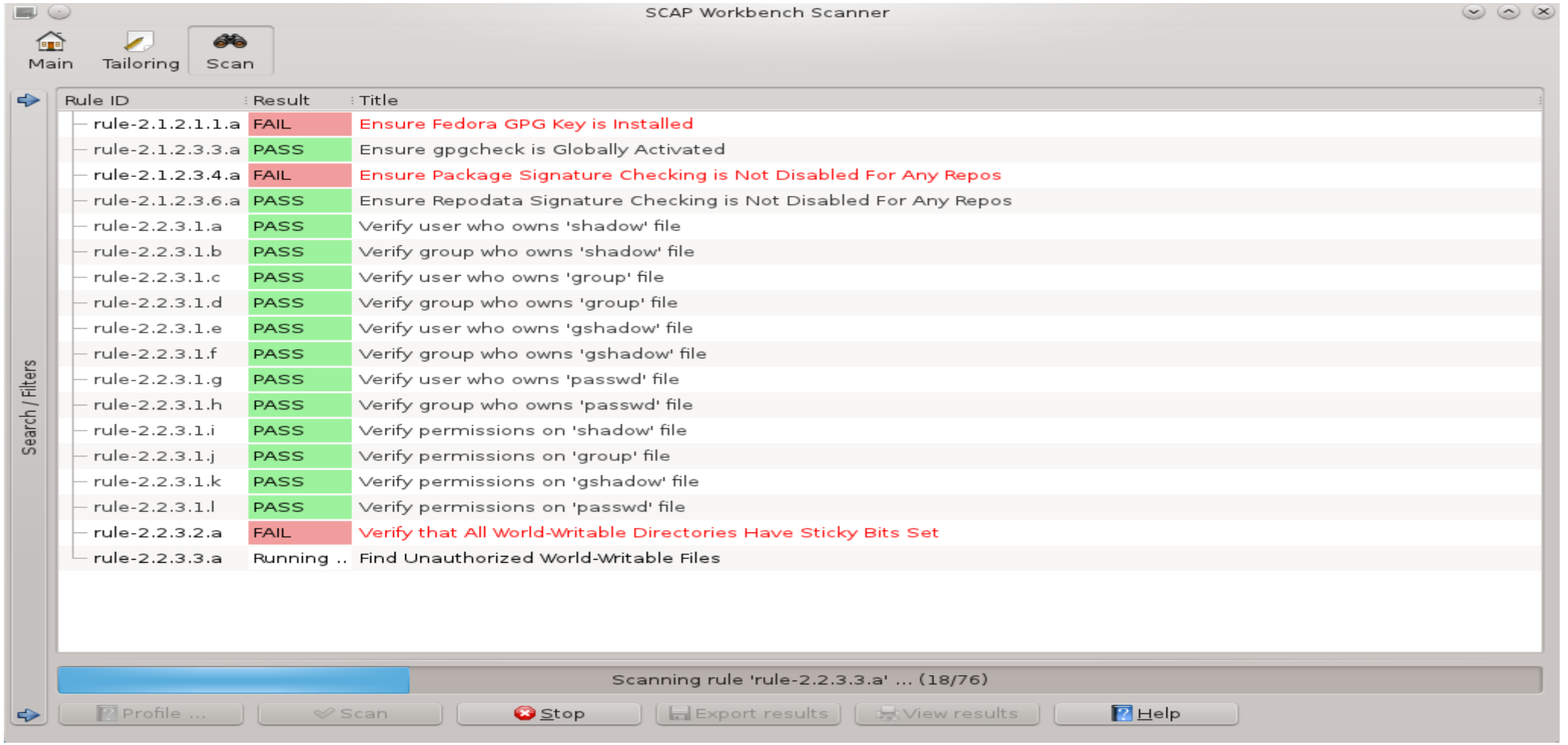
Oval Definition Results

True | False | Error | Unknown | Not Applicable | Not Evaluated

OVAL ID	Result	Class	Reference ID	Title
oval:tutorial:def:1	true	compliance		SELinux Policy Installed

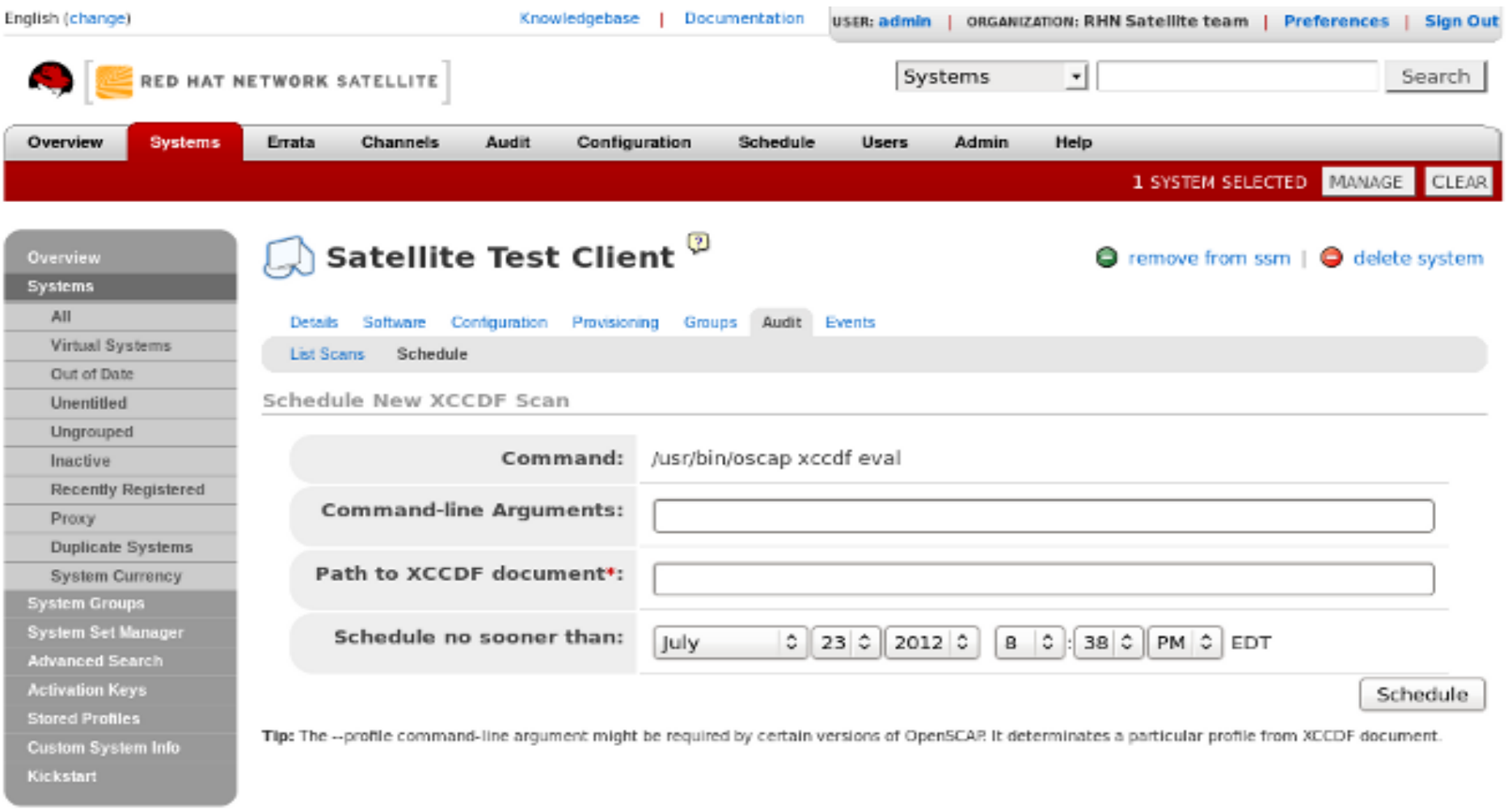
OpenSCAP Frontends

- Enhanced SCAP editor (Content editor)
- SCAP-workbench (Content editor und scanner)



redhat

Integration in System Management Tools



redhat

OpenSCAP Ressourcen

- OpenSCAP
  - http://open-scap.org
- SCAP Security Guide (SSG)
  - http://fedorahosted.org/scap-security-guide
- RHEL6 STIG
  - http://iase.disa.mil/stigs/os/unix/red_hat.html
- eSCAPe
  - http://sourceforge.net/projects/escapeditor/
- scap-workbench
  - http://fedorahosted.org/scap-workbench/
- OVAL Repository
  - http://oval.mitre.org/repository/about/other_repositories.html

redhat

Zusammenfassung

- OpenSCAP ist ein Scanning-Tool zum automatischen Scannen von Systemen
- Es werden System-Konfigurationen und Software-Stände überprüft
- Es existiert freier Content in grosser Anzahl
- Hersteller liefern OVAL-Daten
- Content ist modular aufgebaut und lässt sich leicht wiederverwerten und bei Bedarf anpassen
-