Martin Preisler

@MartinPreisler
Senior Software Engineer
mpreisle@redhat.com

OPENSCAP

open-source SCAP 1.2 implementation

- security automation
- SCAP = Security Content Automation Protocol
- certified by NIST since 2014
- library and a command-line interface
- GUI frontend is available - *SCAP Workbench*

OpenSCAP BASE

SCAP WORKBENCH

SCAP SECURITY GUIDE

open-source SCAP security policy project

- community project
- content for multiple products - RHEL, Fedora, CentOS, Firefox, ...
- multiple policies for each product - USGCB, PCI-DSS, DISA STIG, ...

TWO TYPES OF SCAP SECURITY POLICIES

VULNERABILITY ASSESSMENT

detect CVEs

Heartbleed

Shellshock

Ghost

VENOM

...

SECURITY COMPLIANCE

proper configuration

hardening

USGCB

PCI-DSS

DISA STIG

...

TWO SCAP USE-CASES

VULNERABILITY ASSESSMENT

are my machines vulnerable to:

Heartbleed?

Shellshock?

Ghost?

VENOM?

...?

SECURITY COMPLIANCE

is root login over ssh forbidden?

is SELinux enabled and enforcing?

are we using strict password policy?

are obsolete / insecure services disabled?

...?

SCAP CONSUMERS

VULNERABILITY ASSESSMENT

Everybody who has an attack surface

SECURITY COMPLIANCE

Regulatory:

- Government agencies, contractors
- Financial companies
- Health care, Energy
- ...

Pro-active security

DEMO 1:
AUTOMATICALLY CHECK VULNERABILITIES

DEMO 2:
SECURITY COMPLIANCE

DEMO 3:
CONTAINERS

DEMO 4:
COMPLIANCE VIA ANSIBLE