Uses Machine Learning for Security Compliance

Author: Jan Rodák

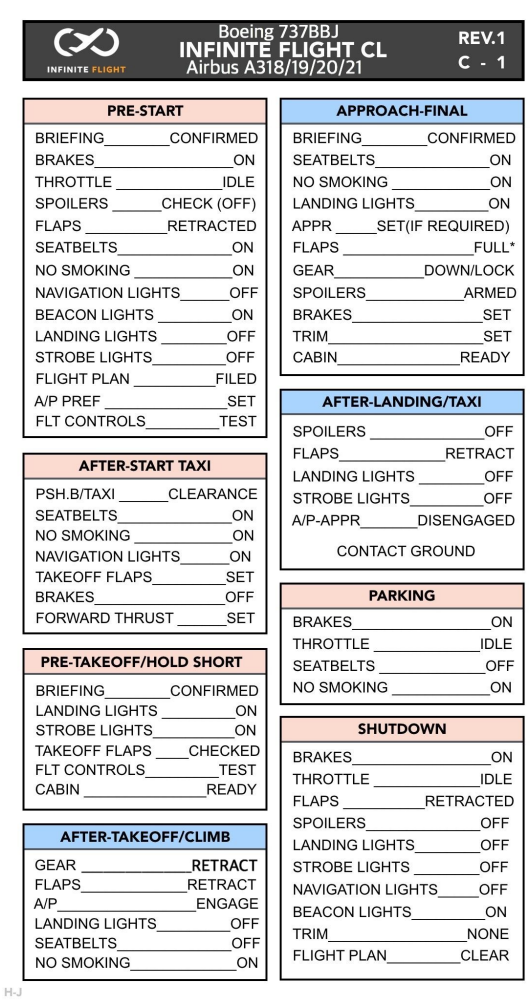
Red Hat

Outline

- What is security compliance
- SCAP standard
- OpenSCAP ecosystem
- From Security Policy to scan
- Why rule filed

Security Compliance

- Active steps an organization takes to protect its assets
- Meet internal security and/or legal requirements
- Check list of rules



INFINITE FLIGHT

Boeing 737BBJ
INFINITE FLIGHT CL
Airbus A318/19/20/21

REV.1
C - 1

PRE-START

BRIEFING _____ CONFIRMED
BRAKES _____ ON
THROTTLE _____ IDLE
SPOILERS _____ CHECK (OFF)
FLAPS _____ RETRACTED
SEATBELTS _____ ON
NO SMOKING _____ ON
NAVIGATION LIGHTS _____ OFF
BEACON LIGHTS _____ ON
LANDING LIGHTS _____ OFF
STROBE LIGHTS _____ OFF
FLIGHT PLAN _____ FILED
A/P PREF _____ SET
FLT CONTROLS _____ TEST

AFTER-START TAXI

PSH.B/TAXI _____ CLEARANCE
SEATBELTS _____ ON
NO SMOKING _____ ON
NAVIGATION LIGHTS _____ ON
TAKEOFF FLAPS _____ SET
BRAKES _____ OFF
FORWARD THRUST _____ SET

PRE-TAKEOFF/HOLD SHORT

BRIEFING _____ CONFIRMED
LANDING LIGHTS _____ ON
STROBE LIGHTS _____ ON
TAKEOFF FLAPS _____ CHECKED
FLT CONTROLS _____ TEST
CABIN _____ READY

AFTER-TAKEOFF/CLIMB

GEAR _____ **RETRACT**
FLAPS _____ RETRACT
A/P _____ ENGAGE
LANDING LIGHTS _____ OFF
SEATBELTS _____ OFF
NO SMOKING _____ ON

APPROACH-FINAL

BRIEFING _____ CONFIRMED
SEATBELTS _____ ON
NO SMOKING _____ ON
LANDING LIGHTS _____ ON
APPR _____ SET(IF REQUIRED)
FLAPS _____ FULL*
GEAR _____ DOWN/LOCK
SPOILERS _____ ARMED
BRAKES _____ SET
TRIM _____ SET
CABIN _____ READY

AFTER-LANDING/TAXI

SPOILERS _____ OFF
FLAPS _____ RETRACT
LANDING LIGHTS _____ OFF
STROBE LIGHTS _____ OFF
A/P-APPR _____ DISENGAGED

CONTACT GROUND

PARKING

BRAKES _____ ON
THROTTLE _____ IDLE
SEATBELTS _____ OFF
NO SMOKING _____ ON

SHUTDOWN

BRAKES _____ ON
THROTTLE _____ IDLE
FLAPS _____ RETRACTED
SPOILERS _____ OFF
LANDING LIGHTS _____ OFF
STROBE LIGHTS _____ OFF
NAVIGATION LIGHTS _____ OFF
BEACON LIGHTS _____ ON
TRIM _____ NONE
FLIGHT PLAN _____ CLEAR

H-J

Red Hat

SCAP standard

- Security Content Automation Protocol (SCAP)
- SCAP Components
  - **XCCDF** - The Extensible Configuration Checklist Description Format
  - **OVAL** - Open Vulnerability and Assessment Language
  - **ARF** - Asset Reporting Format
  - etc.

XCCDF

- Language for writing checklist
  - Profile selection of rules
  - Rules
- Structured collection of security configuration rules for some set of target systems

OVAL

- Main component of the SCAP standard
- Security vulnerabilities
- Desired configuration of systems
- Define a state of some objects in a computer
  - Configuration files
  - File permissions
  - Processes

OVAL

Definition

```
<definition id="oval:ssg-service_auditd_enabled:def:1" version="1" class="compliance">
  <metadata>
    <title>Enable auditd Service</title>
    <affected family="unix">
      <platform>Fedora</platform>
    </affected>
    <reference source="ssg" ref_id="service_auditd_enabled"/>
    <description>The auditd service should be enabled if possible.</description>
  </metadata>
  <criteria comment="package audit installed and service auditd is configured to start">
    <criterion test_ref="oval:ssg-test_service_auditd_package_audit_installed:tst:1" comment="audit installed"/>
    <criteria comment="service auditd is configured to start and is running">
      <criterion test_ref="oval:ssg-test_service_running_auditd:tst:1" comment="auditd is running"/>
      <criteria operator="OR" comment="service auditd is configured to start">
        <criterion test_ref="oval:ssg-test_multi_user_wants_auditd:tst:1" comment="multi-user.target wants auditd"/>
        <criterion test_ref="oval:ssg-test_multi_user_wants_auditd_socket:tst:1" comment="multi-user.target wants auditd socket"/>
      </criteria>
    </criteria>
  </criteria>
</definition>
```

OVAL

Test

```
<linux:systemdunitproperty_test id="oval:ssg-test_service_running_auditd:tst:1"
check="at least one" check_existence="at_least_one_exists" comment="Test that the auditd service is running" version="1">
  <linux:object object_ref="oval:ssg-obj_service_running_auditd:obj:1"/>
  <linux:state state_ref="oval:ssg-state_service_running_auditd:ste:1"/>
</linux:systemdunitproperty_test>
```

Object

```
<linux:systemdunitproperty_object id="oval:ssg-obj_service_running_auditd:obj:1" comment="Retrieve the ActiveState property of auditd" version="1">
  <linux:unit operation="pattern match">^auditd\.(socket|service)$</linux:unit>
  <linux:property>ActiveState</linux:property>
</linux:systemdunitproperty_object>
```

State

```
<lin-def:systemdunitproperty_state id="oval:ssg-state_service_running_auditd:ste:1" version="1" comment="auditd is running">
  <lin-def:value>active</lin-def:value>
</lin-def:systemdunitproperty_state>
```

OpenSCAP ecosystem

- Implementation of the SCAP standard
- OpenSCAP Base (Library)
- OpenSCAP Scanner
- SCAP Security guide (Content)
- Other tools

Red Hat

From Policy to Scan (Idea 1)

Policy is developed by some organization for example FBI. (https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center)

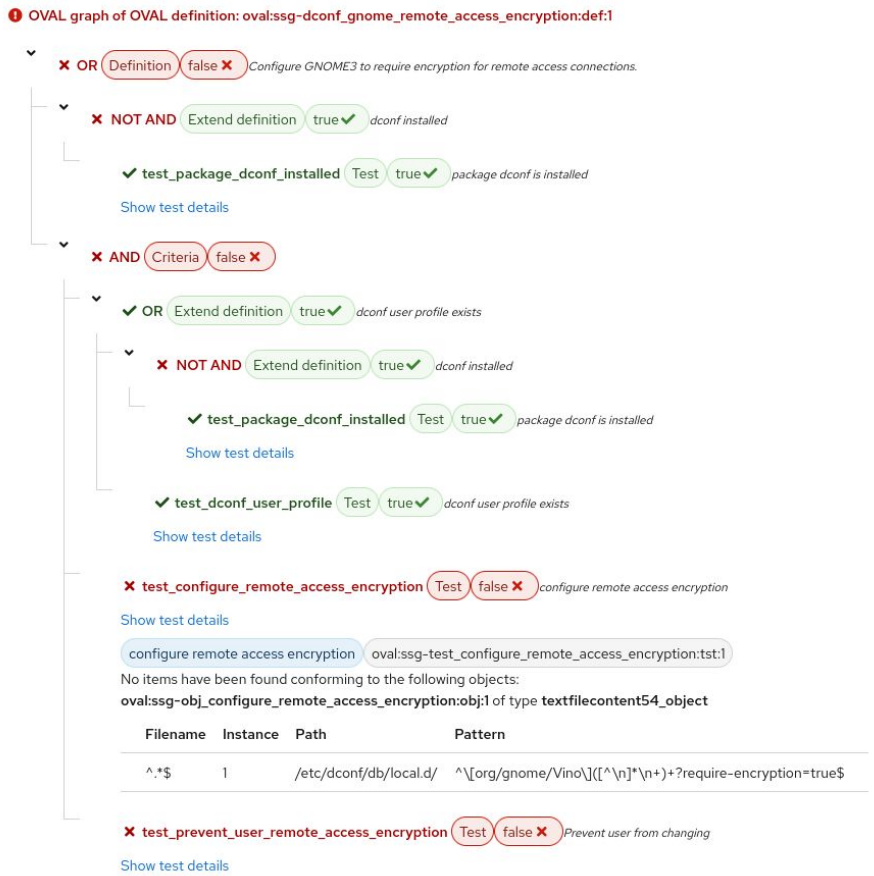
Selection of rules from content based on given policy. (https://complianceascode.github.io/content-pages/guides/ssg-rhel8-guide-cjis.html)

Compiling all components of SCAP to one file named DataStream.

Output is ARF file.

Why is rule fail (Idea 2)

- SCAP content provides OVAL for many cases
- Remediation just for one case



Red Hat

Bibliography

[1] *OVAL Content Creation Tutorial*. Center for Internet Security, 2017 [cit. 2023-11-18]. Available at: https://ovalproject.github.io/getting-started/tutorial/.

[2] T*he Security compliance content in SCAP, Bash, Ansible, and other formats* [online]. 2022 [cit. 2022-11-18]. Available at: https://github.com/ComplianceAsCode/content.

[3] Waltermire, D., Quinn, S., Booth, H., Scarfone, K. and Prisaca, D. *The Technical Specification for the Security Content Automation Protocol (SCAP)*. NIST Special Publication 800-126, 3rd ed. National Institute of Standards and Technology, february 2018 [cit. 2022-11-18]. Available at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-126r3.pdf.

Thank You for Your Attention!