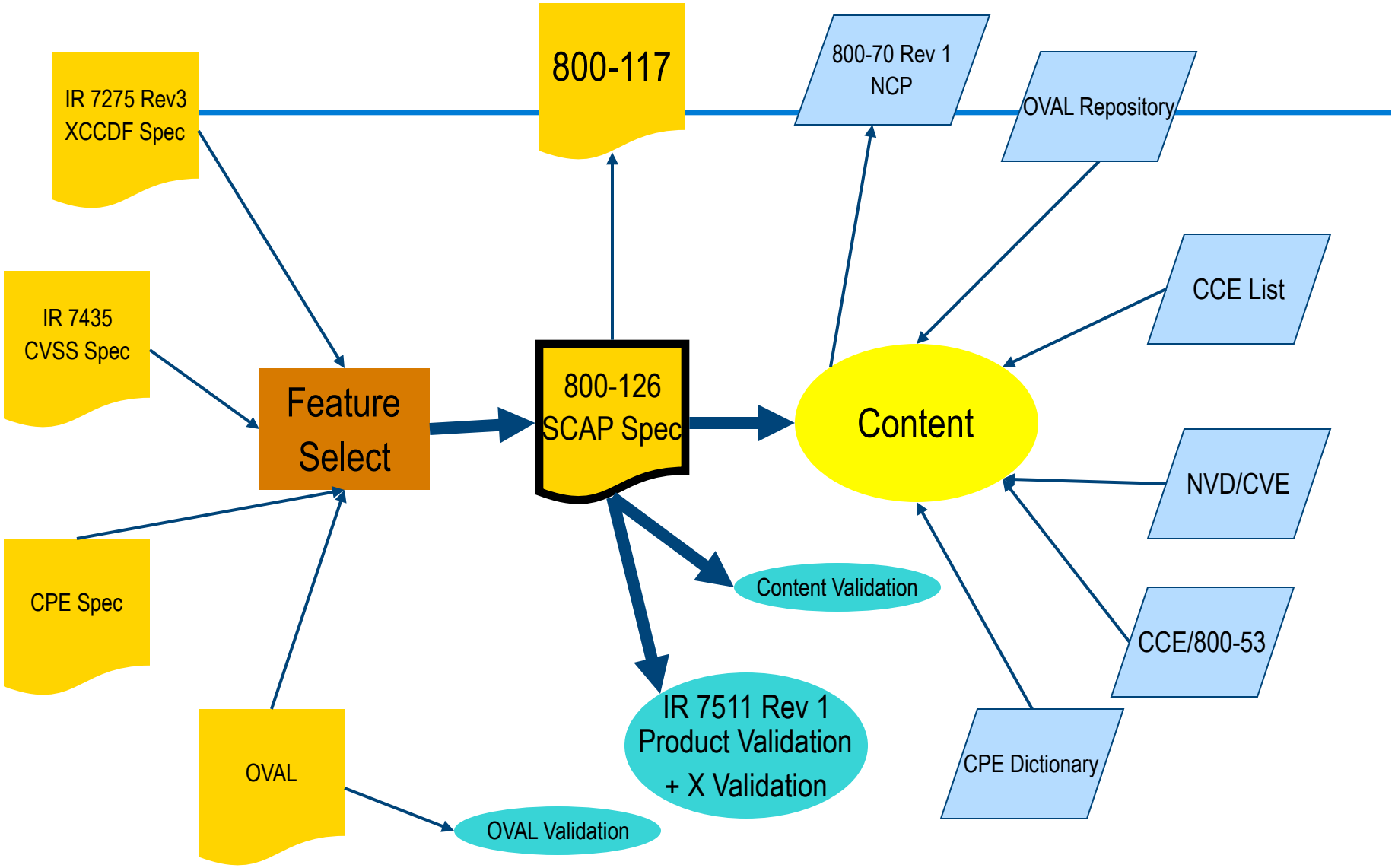
# NIST SP 800-126 Review


The technical specification for SCAP version 1.0

Presented by:
David Waltermire

# Document and Data Relationships



# Purpose

- Describes the current version of SCAP, 1.0
- Documents history, what SCAP is today
- Documents the interrelationships of the SCAP component specifications
- Documents conventions and requirements that are not defined in the individual component specifications
- Defines the characteristics of SCAP content for producers and consumers
- Expresses common SCAP use-cases

# Document Organization

- Section 2: Overview
- Section 3: SCAP Component Basics
- Section 4: General Requirements and Conventions (Interrelationships)
- Section 5: Use-Case Requirements

# Section 3: Basics of SCAP Components

- Categories
  - Languages (XCCDF, OVAL)
  - Enumerations (CPE, CCE, CVE)
  - Metric (CVSS)
- Brief overview of each specification
- Links to related resources
- Rough content examples
- Relationship to other specs

# Section 3: Basics of SCAP Components (Continued)

- Does this section provide too little/much information on each specification?
- Are there other specification related resources/references that should be provided?

# Section 3: Basics of SCAP Components (Continued)

- Enumerations vs. Identifiers
  - What is the difference?
  - Do current SCAP enumerations break the mold?
    - Standardized nomenclature
    - Semantic definitions
  - What data should accompany identifiers as part of the specification?
    - Should references be allowed?
    - What references?
  - Should identifier based data feeds exist as a language specification?

# Section 3: Basics of SCAP Components (Continued)

- Any additional comments?

# Section 4: SCAP General Requirements and Conventions

- Use of IETF RFC 2119 to indicate convention verses requirement
- Conventions – Best practice guidance that applies to content and products without regard to use-case
- Requirements – Rules that must be followed for all use-cases

# Section 4.1: XCCDF General Requirements and Conventions

- Should there be SCAP requirements or conventions for the use of Groups?
  - Level of abstraction
  - Nesting
- Should there be SCAP requirements or conventions for Rule identifier naming?
  - Auto vs. Hand generated concerns
  - Should identifiers imply meaning?

# Section 4.1: XCCDF General Requirements and Conventions (Continued)

- Should CPE Names be allowed on Rules, Groups and Profiles?
- Should the usage of complex checks be allowed in SCAP content? Or should we provide guidance on referencing a single OVAL definition per Rule?

# Section 4.1: XCCDF General Requirements and Conventions (Continued)

- Should the <indentity> element be required on <TestResult> elements?

```
<cdf:TestResult …>
    …
    <cdf:identity authenticated="1“ privileged="1">admin_bob</
    cdf:identity>
    …
</cdf:TestResult>
```

# Section 4.1: XCCDF General Requirements and Conventions (Continued)

- What content should be required for the <target> element?

```
<cdf:TestResult …>
    …
    <cdf:target>lower.test.net</cdf:target>
    <cdf:target-address>192.168.248.1</cdf:target-address>
    <cdf:target-address>2001:8::1</cdf:target-address>
    <cdf:target-facts>
        <cdf:fact type="string" name="urn:scap:fact:asset:identifier:mac">02:50:e6:c0:14:39</
    cdf:fact>
        <cdf:fact type="string" name="urn:scap:fact:asset:identifier:host_name">lower</
    cdf:fact>
        <cdf:fact type="string" name="urn:scap:fact:asset:identifier:ipv4">192.168.248.1</
    cdf:fact>
        <cdf:fact type="string" name="urn:scap:fact:asset:identifier:ipv6">2001:8::1</cdf:fact>
    </cdf:target-facts>
    …
</cdf:TestResult>
```

# Section 4.1: XCCDF General Requirements and Conventions (Continued)

- Possible <target-facts>:
  - **urn:scap:fact:asset:identifier:mac**
  - **urn:scap:fact:asset:identifier:ipv4**
  - **urn:scap:fact:asset:identifier:ipv6**
  - **urn:scap:fact:asset:identifier:host_name**
  - **urn:scap:fact:asset:identifier:fqdn**
  - **urn:scap:fact:asset:identifier:ein**
  - **urn:scap:fact:asset:identifier:pki:**
  - **urn:scap:fact:asset:identifier:pki:thumbprint**
  - **urn:scap:fact:asset:identifier:guid**
  - **urn:scap:fact:asset:identifier:ldap**
  - **urn:scap:fact:asset:identifier:active_directory**
  - **urn:scap:fact:asset:identifier:nis_domain**
  - **urn:scap:fact:asset:environmental_information:owning_organization**
  - **urn:scap:fact:asset:environmental_information:current_region**
  - **urn:scap:fact:asset:environmental_information:administration_unit**
  - **urn:scap:fact:asset:environmental_information:administration_poc:title**
  - **urn:scap:fact:asset:environmental_information:administration_poc:e-mail**
  - **urn:scap:fact:asset:environmental_information:administration_poc:first_name**
  - **urn:scap:fact:asset:environmental_information:administration_poc:last_name**
- Are others needed?

# Section 4.2: OVAL General Requirements and Conventions

- Should compliance and inventory definitions be segregated to provide granularity in result reporting?

```
<definition id="oval:org.mitre.oval:def:6092" version="0" class="vulnerability">
    …
    <criteria operator="AND" comment="Solaris 8 (SPARC) meets Sun Alert 259468">
       <extend_definition comment="Solaris 8 (SPARC) is installed"
    definition_ref="oval:org.mitre.oval:def:1539"/>
       <criterion negate="true" comment="Patch 116455-02 or later installed"
    test_ref="oval:org.mitre.oval:tst:9833"/>
    </criteria>
    <criteria operator="AND" comment="Solaris 9 (SPARC) meets Sun Alert 259468">
       <extend_definition comment="Solaris 9 (SPARC) is installed"
    definition_ref="oval:org.mitre.oval:def:1457"/>
       <criterion negate="true" comment="Patch 116453-03 or later installed"
    test_ref="oval:org.mitre.oval:tst:9695"/>
    </criteria>
    …
</definition>
```

# Section 4.2: OVAL General Requirements and Conventions

- Should a vulnerability definition be allowed to extend a compliance definition?

# Section 4: SCAP General Requirements and Conventions

- Any additional comments?

# Section 5: SCAP Use-Case Requirements

- Specific requirements based on use-case
- Use Cases
  - Configuration Verification (XCCDF and OVAL)
  - Vulnerability Assessment
    - XCCDF and OVAL
    - Standalone OVAL
  - Inventory Collection

# Section 5: SCAP Use-Case Requirements

- Any additional comments?

# Contact Information

David Waltermire

david.waltermire@nist.gov

http://scap.nist.gov/