Extensible Configuration Checklist Description Format (XCCDF)

The standard for expressing security and configuration guidance for computer systems

XCCDF is the standard language for authoring information security benchmarks, checklists, and other configuration guidance. Each XCCDF document, written in Extensible Markup Language (XML), includes: prose information about guidance regarding a particular policy or set of policies, links to technical mechanisms to evaluate this guidance, and the ability to store results of assessments against that guidance. When used with checking languages, such as the Open Checklist Interactive Language (OCIL) and Open Vulnerability and Assessment Language (OVAL®) standards, XCCDF can also be used to perform automated system assessments. Assessment results are expressed in an XCCDF results format that can be stored for recordkeeping or used by software products for processing and remediation.

XCCDF Benefits

- Standard format for authoring security guidance
- Compatible with checking languages
- Enables storage and transmission of assessment results
- Convertible to human-readable documentation
- Enables interoperability between tools
- Supports automation of the assessment process

MITRE's Role

XCCDF is published by the U.S. National Institute of Standards and Technology (NIST).

MITRE Corporation has been closely involved in the development of XCCDF since its inception. Today, MITRE serves as the moderator of the effort, responding to community questions, moderating discussions on the XCCDF Discussion List and in community meetings, managing updates to the XCCDF interpreter, presenting XCCDF information at security automation conferences and other events, and contributing to revisions of the specification document and schema.

Why XCCDF

Prior to XCCDF, security configuration guidance benchmarks and checklist documents were primarily prose-based and stored in diverse non-digital and digital formats. As a result, implementing the corresponding guidance on a system generally involved interpretation on the part of the implementer, which could sometimes lead to inconsistencies. In addition, the results of the software policy checks were often rendered in a proprietary format that could not be processed or exchanged among software products from different vendors, severely restricting use of the data and the potential of interoperability. XCCDF addresses these problems.

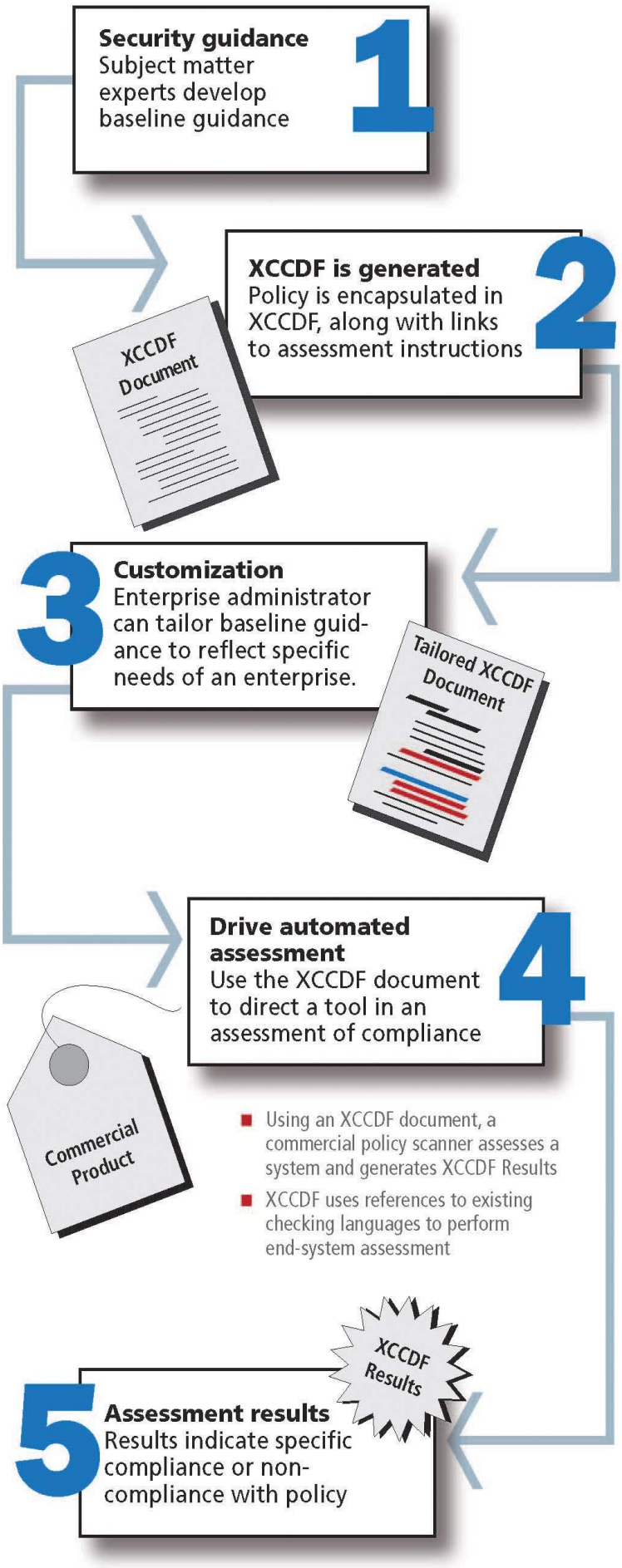
Using XCCDF

XCCDF supports several use cases and capabilities that are of interest to those who must create, publish, test, and record results for enterprise security policies.

- **Authoring security configuration guidance** – Creating XCCDF content requires no special tools. As a result organizations can easily use XCCDF to encapsulate their internal software policies so they can then be supported by XCCDF-compatible tools.
- **Document generation** – Policies encapsulated in an XCCDF document can be exported to a human-readable document using simple procedures.
- **Compliance testing** – XCCDF can guide automated policy assessment of end system using any XCCDF-compliant tool.
- **Reporting** – Results of XCCDF compliance tests use a detailed, standardized format that can be used for aggregation, analysis, and trending in a vendor-neutral way.
- **Tailoring** – XCCDF supports tailoring activities by end users, allowing content to be quickly customized to specific needs of individual enterprises.

As use of XCCDF becomes more widespread via community development of XCCDF-compatible tools, XCCDF will further complement security automation efforts such as Security Automation Protocol (SCAP) and other efforts seeking to improve and automate the cyber security ecosystem. XCCDF is a main component of SCAP, which uses XCCDF, OVAL, OCIL, and other existing standards to enable enterprise solutions for automated vulnerability management, measurement, and policy compliance.

How XCCDF Works



Written in XML, an XCCDF document represents a structured collection of security configuration rules for some set of target systems. Many tools are available to help develop and apply XCCDF documents including two that are free to download and use: an XCCDF Interpreter reference implementation and a specialized editor called Recommendation Tracker.

XCCDF Interpreter

Managed by MITRE, the XCCDF Interpreter is a standalone Java reference implementation that demonstrates how an XCCDF Document can be evaluated. The interpreter can be used to test XCCDF content, demonstrate canonical behavior of XCCDF interpreters, and to perform basic system assessments using XCCDF and OVAL content. The interpreter and its source code are free to download at *http://sourceforge.net/projects/xccdfexec/*.

Recommendation Tracker™

MITRE's Recommendation Tracker can be used to simplify the creation of XCCDF content. Recommendation Tracker allows users to create policies using a wizard-like interface that can then be directly exported to XCCDF for use with XCCDF-compatible tools. Recommendation Tracker and its source code are available for free download at *http://sourceforge.net/projects/rectracker/*.

Community Participation Needed

Community participation is integral to the success of XCCDF. We encourage members of the information security community to participate in the XCCDF effort by joining the XCCDF Developer's Email Discussion list to discuss and offer feedback on the XCCDF Specification and XCCDF Schema at *xccdf-dev@nist.gov*.

Learn More

http://scap.nist.gov/specifications/xccdf/

XCCDF
security benchmark automation