Open Checklist Interactive Language (OCIL™)

A standardized approach for expressing and evaluating non-automated security checks

OCIL provides a standardized framework for collecting information from people so that their responses are machine-readable for processing by software products. Created for the purpose of developing security checklists, OCIL includes standardized Extensible Markup Language (XML) constructs for representing questions, instructions that guide users towards an answer, and a final result that can be processed immediately or stored digitally for later use. OCIL can also be used to convert legacy security information into a standardized format, thus enabling new uses and data mining opportunities. OCIL also enables interoperability between security products by allowing them to exchange information through a standard XML language.

MITRE's Role

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

MITRE Corporation wrote the initial versions of the OCIL Language Specification document and OCIL Schema, and has contributed to all subsequent drafts. MITRE also developed the reference implementation of the OCIL Interpreter currently available for free download.

MITRE continues to support the OCIL effort on an ongoing basis by responding to community questions, moderating discussions on our OCIL Discussion List, presenting OCIL information at security automation conferences and other events, planning an adoption program for OCIL-compatible software tools, and contributing to revisions of the specification document and schema for future releases.

OCIL Benefits

- Provides a common language for manual security checks
- Consistency in check evaluation
- Interoperability between tools
- Ability to share documents between authors
- Enables the ability to audit evaluation results and inspect user responses

Why OCIL

Until OCIL, the manual components of assessing security controls related to people and processes were often recorded in diverse formats, making it difficult to share data across an organization or with other organizations. And when the same format was used, individual users would record answers differently. In addition, the results of these assessments were often not rendered in a format that could be processed or exchanged among software products that were not proprietary, severely restricting use of the data and the potential of interoperability and automation. OCIL solves these problems.

OCIL in Use

A reference implementation of an OCIL Interpreter is available now. Once this functionality is more widespread via community development of OCIL-compatible tools, OCIL will further complement security automation efforts such as Security Automation Protocol (SCAP) and other efforts seeking to improve and automate the cyber security ecosystem.

OCIL, which is included in SCAP Version 1.2, can be used now in the following ways for expressing and evaluating non-automated security checks:

• **Supplementing automated system security checks** – OCIL can be used when manual human input is required in system assessment such as using an XCCDF Document to specify system checks for demonstrating PCI-DSS compliance. The XCCDF Document will reference an OCIL Document when a step calls for a manual check, which will be presented to the user as a series of questions. OCIL Interpreter functionality will collect the response(s) and interpret the results, which will then be aggregated into a single report by an XCCDF interpreter to demonstrate compliance.

• **Aggregating security data from multiple data sources** – OCIL can be used to harvest data from multiple sources, such as system configuration management information located in various databases, and store it in a standardized XML-based format. This aggregated information can then be combined with other XML-based sources, such as the results of OVAL checks, for more comprehensive evaluation or other uses.

• **Repurposing previously collected security data** – Information collected for a different purpose and stored in a database can be leveraged in new ways using OCIL, for instance with copies of configuration files from systems recently collected for a different purpose. To determine which systems have a particular configuration, pertinent information in the database can be harvested through automated techniques and then used by an OCIL Document to determine which systems have the specified configuration file. Copies of those configuration files can then be transferred elsewhere, such as to a central server, for subsequent review and action.

How OCIL Works

The basic entity in OCIL for users is an OCIL Document written in XML. There is one OCIL Document for all of the questions you wish to pose, as for example in a survey. OCIL Documents are comprised of three primary object groups: questionnaires, test actions, and questions. "Questionnaires" are the top-level objects that are referred to externally for users. A questionnaire will reference one or more test actions. A "Test Action" is what determines the workflow or the sequence of questions presented to the end user. The "Questions," which can be one of four types, can be referenced by multiple test actions. The questions contain the verbiage shown to the user. Users' responses are output in machine-readable format and those results can lead to an action, be issued in a report, or be combined with other XML-based sources for other security-related purposes.

OCIL Document Features

• **One OCIL Document for all user-composed questions** – Each document contains one or more of your top-level questions seeking to determine a state or condition. The same document records the eventual computed answer, which may also include additional information or attachments.

• **Each document constructed to guide respondent to an answer** – Document's top-level questions, which seek to determine a state or condition, invoke pre-defined sub-question(s) that lead to a new sub-question or to the final answer.

• **Four question categories available** – (1) questions answered by yes/no or true/false; (2) questions answered by selecting one answer from a provided list; (3) questions answered with a numeric value such as a barcode number; or, (4) questions answered with a text string of any combination of letters, numbers, spaces, and punctuation.

• **Ability to accept physical attachments** – Text, reference to a document or URL, or some other physical item may be submitted in support of a response to a question.

• **Final outcome is machine-readable** – Document's output result is ready for immediate processing by software incorporating an OCIL Interpreter, or can be stored for later processing.

• **Unique identifiers for tracking** – Each document has its own identifier, as does each subsection item within the document including the respondent's answer and each attachment, if any.

OCIL Interpreter

Developed by MITRE, the OCIL Interpreter is a standalone Java GUI reference implementation that demonstrates how an OCIL Document can be evaluated. It guides the end user in completing questionnaires one question at a time, and viewing and computing results. The interpreter is free to download at *http://sourceforge.net/projects/interactive/?abmode=1*.

Relationship to Existing Security Assessment Standards

Open Vulnerability and Assessment Language (OVAL®) is an industry standard language for determining the machine state of a computer system through XML-based checks that can be automated. OCIL can be used in conjunction with OVAL when portions of an assessment cannot be automated and require operator input for certain questions. In addition, both OVAL and OCIL produce XML-based output so results can be combined to produce a report or lead to an action.

Extensible Configuration Checklist Description Format (XCCDF) is an XML-based specification language for expressing security configuration checklists and other sets of system assessment rules that point to other XML documents, such as OVAL and OCIL documents, which contain the actual instructions for performing the checks.

Community Participation Needed

Community participation is integral to the success of OCIL. We encourage members of the information security community to participate in the OCIL effort by offering feedback and discussing the OCIL Specification and OCIL Schema at *http://scap.nist.gov/community.html#emaillist-emerging-specs*.

Learn More

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