HOW OVAL WORKS

Configuration policy

Government agencies such as NSA and NIST develop "Best Practices" policy for system security.

(1)

Security advisories

CERT-CC, US-CERT, and other organizations publish security advisories that warn of current threats and system vulnerabilities.

(2) Definitions are generated

Specific machine configuration details from Advisory and Policy documents are extracted and encoded as an OVAL Definition.

OVAL Definitions

OVAL System Characteristics

Commercial Product

A commercial vulnerability scanner can read OVAL Definitions and use them to gather configuration information to generate a system characteristics file.

(3) Data collected from computers

OVAL Definitions are structured to indicate what configuration information needs to be collected from an individual system.

OVAL Analysis

Current state → Vulnerable state
Current state ← Vulnerable state

(4) Analysis

The OVAL Definitions from Step 2, and the System Characteristics from Step 3 are compared to determine if the current system state is vulnerable or not vulnerable.

Commercial Product

Using the Definitions and System Characteristics files, a commercial vulnerability scanner performs the OVAL Analysis and generates OVAL results.

OVAL Results

(5) Analysis results

Results of analysis are formatted as an OVAL Results document.
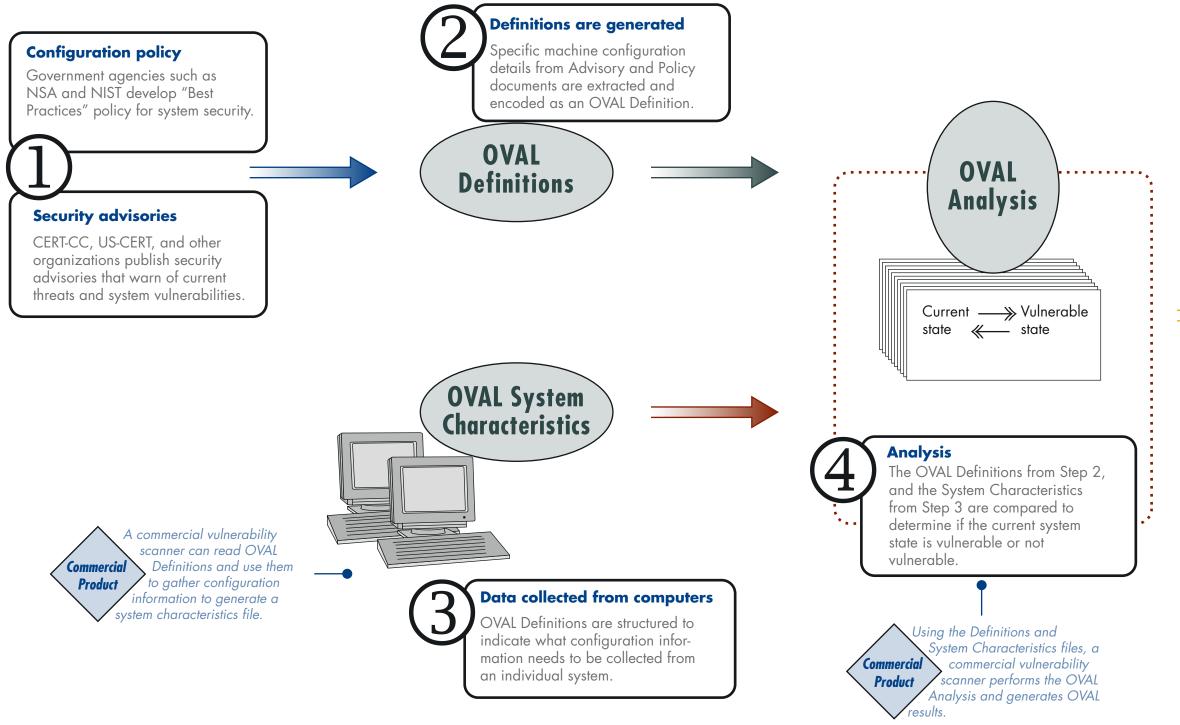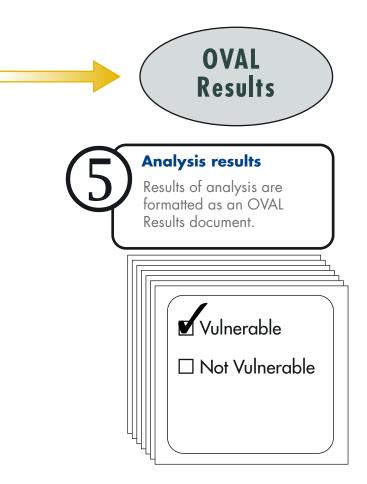
☑ Vulnerable
☐ Not Vulnerable

OVAL
oval.mitre.org

Open Vulnerability and Assessment Language