UALYS®
CONTINUOUS SECURITY

SCAP — Security Content Automation Protocol

Qualys SCAP Auditor 1.2

The Security Content Automation Protocol (SCAP) is a U.S. Government standard for automating vulnerability management and policy compliance with mandated security configurations for personal computers used by federal agencies. Vulnerability scanners used by federal agencies must be validated for SCAP compliance.

About SCAP

SCAP incorporates six open standards for finding vulnerabilities and misconfigurations related to security. It focuses on automating these processes, scoring results, and prioritizing their impact. The goal is to automatically check the security configuration status of an agency's installed base of personal computers against the NIST Special Publication 800-53 controls framework to ensure secure computing. This framework was created by the National Institute of Standards and Technology under mandate of FISMA — the Federal Information Security and Management Act.

SCAP plays a central role in the Federal Desktop Core Configuration (FDCC) Initiative, which, since February 1, 2008, has mandated standard security configurations for agencies using, or planning upgrades to Microsoft Windows XP and VISTA operating systems. The Office of Management and Budget issued this statement to federal Chief Information Officers on July 31, 2007: "Information technology providers must use SCAP validated tools, as they become available, to certify their products do not alter these configurations, and agencies must use these tools when monitoring use of these configurations."

Subsequently in May 2010, the standard was updated for Windows 7 and Internet Explorer 8 and released as the “United States Government Configuration Baseline (USGCB).” The USGCB replaces the Federal Desktop Core Configuration (FDCC) and provides the baseline settings that Federal agencies are required to implement for security and environmental reasons.

Why SCAP Matters to Your Organization

Threats to federal systems and critical cyber infrastructure come from sovereign states, terrorists, criminals, lone hackers, and mistakes committed by staff and contractors. A successful exploit would be disastrous if it stopped vital functions of government and critical services. If a federal agency fails to comply with SCAP, which falls under FISMA, it may be sanctioned via a budget cut. Contractors that exchange data with federal information systems must comply with FISMA-mandated initiatives such as SCAP or risk termination from a contract. Non-compliance may preclude contractors from bidding on future federal contracts.

How Qualys Solutions Help Meet SCAP Requirements

Qualys SCAP Auditor is the first certified cloud-based solution meeting SCAP requirements. Qualys SCAP Auditor allows federal agencies to scan and report compliance with standardized desktop security configuration requirements using a centralized, integrated solution featuring the Qualys Software-as-a-Service (SaaS) architecture. Qualys Scanner Appliances support USGCB scanning for internal systems on a global basis.

Schedule Demo

Compatibility and Certifications

SCAP compliance
Compliant with SCAP version 1.2: XCCDF 1.2, OVAL 5.10, CCE 5, CPE 2.3, CVE, and CVSS 2, OCIL 2.0, CCSS 1.0, Asset Identification 1.1, ARF 1.1, TMSAD 1.0

SCAP 1.2 Certification
Authenticated Configuration Scanner with the CVE option for assessment of Windows 7 (32 and 64 bit) and Red Hat Enterprise Linux (RHEL) 5 Desktop (32 and 64 bit) providing the ability to audit and assess a target system to determine its compliance with USGCB requirements.

Backward Compatibility
SCAP Auditor 1.2 provides backward compatibility with SCAP 1.0 for assessment of Windows XP and Windows Vista supporting USGCB and FDCC assessment.

SCAP Tier III Content
In addition to the SCAP certified assessment capabilities, SCAP Auditor can process SCAP tier III content intended for the following systems: Windows 7 (32 and 64 bit), Windows XP (32 bit), Windows Vista, Windows 2008, Windows 2012, RHEL 5 (32 and 64 bit) and most Linux distributions.

Qualys solutions in the Qualys Security and Compliance Suite also enable immediate compliance with other key FISMA requirements by allowing subscribers to automatically discover and manage all devices and applications on the network, identify and remediate network security vulnerabilities, measure and manage overall security exposure and risk, and ensure compliance with internal and external FISMA policies.

For more details, see the Qualys PC/SCAP Auditor Getting Started Guide.