IBM Endpoint Management (IEM) Security and Compliance - SCAP Implementation Statement

Revision History

Date	Revision	Description	Author
September 20, 2012	**1.0**	**Initial Release**	**Noah Salzman**
September 19, 2014	**1.1**	**SCAP 1.2**	**Shivani Sharma**

SCAP Implementation Statement for IEM Security and Compliance SCAP capabilities:

Authenticated Configuration Scanner - certification for Windows 7 (32/64 bit) OS

Statement of USGCB Implementation

The IEM Security and Compliance product and IEM Platform will run natively within a USGCB hardened environment and requires no change deviations from the USGCB standard on any platform.

However, running the IEM solution may slow down the performance and ability of an IEM agent to receive requests from the server. The IEM agent receives server requests from the server on port 52311. In order for this functionality to work efficiently, the Windows Firewall will need to be modified to allow communication to this port.

If a customer does not open this port, the IEM agent will proactively reach out to the server every 15 minutes, by default, to receive an update and identify anything new. Thus, the solution does not require changes to the USGCB default configuration.

Statement of SCAP 1.2 Implementation

The Security Content Automation Protocol (SCAP) is a method for using specific standards to enable automated vulnerability management, measurement, and policy compliance evaluation.

IEM exists to maintain the health and improve the security of every computing device in the world – fixed or mobile – physical or virtual – through a high-performance, single infrastructure, single console, and single agent solution. Any device, anywhere, anytime! The IEM unified management platform provides high-performance systems and security management solutions for systems lifecycle management, endpoint protection, and security configuration and vulnerability management.

The IEM Security and Compliance product supports the use of SCAP to generate mis-configuration, vulnerability, and patch based assessment rules so organizations can discover and report on software vulnerabilities, assess the impact of those vulnerabilities, enumerate and remediate the mis-configurations identified, and report on the current state of a system based on the SCAP defined policy

definitions. IEM consumes a SCAP-expressed data stream, produces a set of policies known as Fixlet messages, and delivers real-time assessment and remediation on a global scale.

IEM managed systems continuously discover, assess, secure and remediate themselves according to an organization's SCAP-based policies and practices as well as the operating context in which it finds itself – mobile, connected, disconnected, etc. Without requiring significant investments in dedicated hardware, management resources, or professional services, IEM automates enterprise-scale desktop and server management, malware defenses, and IT policy enforcement without compromising network performance, end-user productivity, or security. IEM delivers superior, customer-documented, return-on-investment by reducing labor and infrastructure costs and automating critical management functions.

Statement of CCE 5 Implementation

Common Configuration Enumeration (CCE) 5 provides unique identifiers to system configuration issues in order to facilitate fast and accurate correlation of configuration data across multiple information sources and tools. For example, CCE Identifiers can be used to associate checks in configuration assessment tools with statements in configuration best-practice documents.

IBM is a leading global provider of high-performance systems and security management software for organizations. One of the many features of the Security Configuration and Vulnerability Management solution pack includes the ability to assess workstations, laptops, servers and mobile computing devices against common configuration settings to identify mis-configuration states in a heterogeneous computing environment. IEM fully supports CCE and displays the CCE ID for each mis-configuration for which there is a CCE ID within the IEM Console. In the case where a mis-configuration is associated with multiple CCE IDs all will be cross-referenced and displayed.

Users can easily find the CCE ID associated with a configuration setting by opening the IEM Console and navigating to a configuration setting consumed from an SCAP-expressed data stream, clicking on a Fixlet message that represents a configuration setting, and viewing the Source ID column. The Source ID will display the CCE ID. The CCE ID is also accessible from other views within the product and can be leveraged as part of the reporting criteria for detailed reports and summary reports on individual end-point systems or for a large group of systems reported on in the aggregate.

Statement of CPE 2.3 Implementation

Common Platform Enumeration (CPE) 2.3 is a structured naming scheme for information technology systems, platforms, and packages. Based upon the generic syntax for Uniform Resource Identifiers (URI), CPE includes a formal name format, a language for describing complex platforms, a method for checking names against a system, and a description format for binding text and tests to a name.

IBM is a leading global provider of high-performance systems and security management software for organizations. One of the many features of the Security Configuration and Vulnerability Management solution pack includes the ability to leverage the CPE as a check and balance to ensure that configuration settings are assessed on the correct system. Whether the system is a Windows XP, Vista, 2000, 2003, UNIX or other technology platform, the CPE ID can be used to uniquely identify a given platform and ensure that assessment is done appropriately.

IBM customers can easily optimize the assessment and remediation of system configurations by targeting systems by platform, in addition to numerous other targeting mechanisms. By targeting a particular platform, customers can eliminate the overhead of scanning systems inappropriately and against configuration checks that have no applicability. Configuration checks are assessed in real-time based on the platform and policies can be enforced, enabling administrators to have real-time visibility and control over platforms as needed in a distributed or non-distributed computing environment.

Statement of OVAL 5.10.1 Implementation

The Open Vulnerability and Assessment Language (OVAL) 5.10.1 is an international, information security, community standard to promote open and publicly available security content, and to standardize the transfer of this information across the entire spectrum of security tools and services. The OVAL language is a collection of XML schema for representing system information, expressing specific machine states, and reporting the results of an assessment.

IBM is a leading provider of high-performance systems and security management software for enterprise customers and has been certified as OVAL Compatible since October 2006. Through a repository of vulnerability assessment policies, IBM provides its customers with the ability to assess their managed computers against OVAL vulnerability definitions using real-time data tracking based on the data elements of each definition. These policies are automatically retrieved by the IBM product within an organization's network. Once validated for authenticity, the policies are made available to the IEM client installed on each managed computer and added to their local library of configuration policies. The agent, quietly and continuously evaluates the state of the machine against each policy so that any instance of non-compliance can be immediately reported to the IEM Server for review by an administrator. If pre-authorized by an administrator, the appropriate corrective action will be applied to the computer immediately upon mis-configuration detection — even to remote or mobile users who are not connected to the organization's network.

Statement of XCCDF 1.2 Implementation

The Extensible Configuration Checklist Description Format (XCCDF) 1.2 is a specification language for writing security checklists, benchmarks, and related kinds of documents. An XCCDF document represents a structured collection of security configuration rules for some set of target systems and is the core element to the SCAP-expressed data stream. The specification also defines a data model and format for storing benchmark compliance testing results.

IBM is a leading provider of high-performance systems and security management software for organizations. One of the many features of the Security and Compliance product includes the ability to consume a SCAP-Expressed data stream, which includes the XCCDF component, and translate the underlying configuration checks that are defined into IEM-compatible Fixlet messages. These Fixlet messages enable administrators to assess their computing assets against the SCAP defined configuration rules in real-time across one, thousands, or hundreds of thousands of endpoints regardless of location.

Once the SCAP converted configuration rules are imported into the IEM Console, any system under IEM management control, both on the managed network and off the managed network, can begin to immediately assess themselves against the defined configuration rules. The results of those configuration checks are relayed to the IEM Console where administrators can view the results and generate detailed reports on an individual system or large groups of systems in the aggregate.

IEM also provides the ability to export the results of the configuration checks into the defined XCCDF report format such that the organization can easily store those reports or send the report to another party.

Statement of ARF 1.1 Implementation

The Asset Reporting Format (ARF) 1.1 is a data model to express the transport format of information about assets, and the relationships between assets and reports. The standardized data model facilitates the reporting, correlating, and fusing of asset information throughout and between organizations.

IBM is a leading provider of high-performance systems and security management software for organizations. One of the many features of the Security and Compliance product includes the ability to export results of configuration checks into the Asset Report Format (ARF) such that the organization can easily store those reports or send the report to another party.

Statement of Asset Identification 1.1 Implementation

The Asset Identification 1.1 is a data model for identifying assets, methods for identifying assets, and guidance on how to use asset identification. This specification provides the necessary constructs to uniquely identify assets based on known identifiers and/or known information about the assets. It also identifies a number of known use cases for asset identification.

IBM is a leading provider of high-performance systems and security management software for organizations. One of the many features of the Security and Compliance product includes the ability to export results of configuration checks into the Asset Report Format (ARF) which includes Asset Identification information in the output report XML file.

Statement of SCAP 1.0 and SCAP 1.1 Backwards Compatibility

IEM consumes a SCAP-expressed data stream, produces a set of policies known as Fixlet messages, and delivers real-time assessment and remediation on a global scale. The Security and Compliance product for SCAP 1.2 is backwards compatible with SCAP 1.0 and SCAP 1.1. For SCAP 1.0, the tool is to be used through the “Import Windows SCAP Content” wizard to output XCCDF format. For SCAP 1.1, the content can be consumed by the SCAP 1.2 tool to output SCAP 1.2 Asset Reporting Format (ARF). To use the tool with SCAP 1.2 content, a “--benchmark” flag has been added.

The IEM Security and Compliance product can be used with SCAP 1.0 and 1.1 data streams.
The flags to import SCAP 1.0 and 1.1 content through the SCAP tool are the same as SCAP 1.2 content, except that the “–benchmarks” flag does not need to be specified and the reporting output will be in SCAP 1.2 ARF.

In order to get SCAP 1.0 output in XCCDF form for an SCAP 1.0 data stream, the SCAP 1.0 tool is to be accessed and used through the “Import Windows SCAP Content” wizard.