

# How to Succeed with IT Security Using SCAP

By Ken Halley

**SCAP was developed to respond appropriately to new vulnerabilities and threats and to address the lack of interoperability across system security tools.**

Securing the U.S. against cyber attacks has become one of the nation's top priorities. To achieve this objective, networks, systems, and the operations teams that support them must vigorously defend against external attacks. This also rings true for the commercial sector as more than 70 new vulnerabilities are found each week in commercial applications – and many more have been exploited without public recognition in custom applications written by programmers from individual sites in government, commercial, and private enterprises.

But vulnerabilities are not the only thing on a security executives mind. As more and more vulnerabilities arise, an increasing number of mandates are required. This means an increasing number of frameworks, standards, regulations, and guidelines that the security team must be aware of and prove compliance with.

In 2002, the Cyber Security Research and Development Act tasked the National Institute of Standards and Technology (NIST)<sup>1</sup> to “develop, and revise as necessary, a checklist setting forth settings and option selections that minimize the security risks associated with each computer hardware or software system that is, or is likely to become widely used within the federal government.” Such checklists, when combined with well-developed guidance, leveraged with high-quality security expertise, vendor product knowledge, operational experience, and accompanied with tools, can markedly reduce the vulnerability exposure of an organization.

The most visible of these checklists is the Federal Desktop Core Configuration (FDCC), which leveraged the Security Content Automation Protocol (SCAP).<sup>2</sup> SCAP (pronounced S-Cap) is a method for using specific standards to enable automated vulnerability management, measurement, and policy compliance evaluation. These standards enable products from different vendors to work together to automate the

entire vulnerability management life cycle, which includes vulnerability scanning, patch management, remediation, and policy management.

SCAP was developed to address several problems that exist in security management, namely the need to respond appropriately to new vulnerabilities and threats, prioritizing them so the most significant ones can be addressed sooner. Another problem is the lack of interoperability across system security tools. For example, the use of proprietary names for vulnerabilities creates inconsistencies in reports from multiple tools, which can cause delays in security assessment, decision-making, and vulnerability remediation.

SCAP combines a number of open standards that are used to enumerate software flaws and configuration issues related to security. They measure systems to find vulnerabilities and offer methods to score those findings in order to evaluate the possible impact. It is a method for using those open standards for automated vulnerability management, measurement, and policy compliance evaluation.

There are six underlying SCAP standards:

- **Common Vulnerabilities and Exposures (CVE®)** – a dictionary of names for publicly known security-related software flaws. Currently 33,000 vulnerabilities exist, with more being added each day.
- **Common Configuration Enumeration (CCE™)** – a dictionary of names for software security configuration issues, such as access control settings and password policy settings. These enable faster, more accurate correlation and facilitate information exchange.
- **Common Platform Enumeration (CPE™)** – a naming convention for hardware, operating systems and software.
- **Common Vulnerability Scoring System (CVSS)** – a method for classifying characteristics of software flaws and assigning severity scores.

1 <http://nvd.nist.gov/fdcc/index.cfm>.

2 <http://scap.nist.gov/revision/1.0/index.html> – includes links to individual standards.

- **Extensible Configuration Checklist Description Format (XCCDF)** – an Extensible Markup Language specification for structured collections of security configuration rules used by operating systems and applications.
- **Open Vulnerability and Assessment Language (OVAL™)** – an XML specification for exchanging technical details on how to check systems for security-related software flaws, configuration issues and patches.

While these standards were created by the federal government, SCAP standardization also benefits the commercial markets. In fact, several industry analysts have said that by 2010, more and more commercial entities will begin using SCAP-validated tools. One reason can be found in a recent report from Energy Insights, a division of market research firm IDC, titled “Critical Infrastructure Cybersecurity: Survey Findings and Analysis.” This report documents the challenge of securing the data networks that control critical infrastructure systems. The report, authored by Rick Nicholson, was based on survey data collected from 199 respondents across a number of critical infrastructure industries, such as utilities (electric, gas, and water), oil and gas, financial services, government (federal, state, and local), telecommunications, and transportation. The survey documented that lack of adequate preparation is widespread across critical industry verticals. “The results,” explains Nicholson, “indicate that owners of some of the most critical infrastructure assets, such as utilities, oil and gas companies, transportation companies, chemical companies, and postal/shipping companies are the worst prepared.

## Working with SCAP

Let’s look at how SCAP can address security issues in the commercial market.

### Features and benefits of SCAP include the following:

- Standardizes how computers communicate vulnerability information – enables interoperability for products and services from various manufacturers
- Standardizes what vulnerability information computers communicate – enables repeatability across products and services of various manufacturers and reduces content-based variance in operational decisions and actions
- Based on open standards – harnesses the collective brain power of the masses for creation and evolution and adapts to a wide array of use cases
- Uses configuration and asset management standards – mobilizes asset inventory and configuration information for use in vulnerability and compliance management

- Applicable to many different risk management frameworks (assess, monitor, implement) – reduces time, effort, and expense of risk management
- Detailed traceability to multiple security mandates and guidelines – automates portions of compliance demonstration and reporting and reduces chance of misinterpretation between auditors and operations teams

Managing the configurations and security settings of information systems is a challenging job to do manually because of the size, complexity, and constant changes in the systems. A wide variety of hardware and software platforms typically are used for many purposes with differing levels of risk in a single environment. Most organizations have many systems to patch and configure securely, with numerous pieces of software (operating systems and applications) to be secured on each system. This is extremely time-consuming and error-prone because there has been no standardized, automated way of securing software. SCAP can be used for maintaining the security of enterprise systems, such as automatically verifying the installation of patches, checking system security configuration settings, examining systems for signs of a breach or compromise, identifying the presence of vulnerabilities, and assigning severity scores to software flaws.

Vendors have begun incorporating SCAP standards within their commercial applications because it helps companies demonstrate compliance with high-level security requirements. Security configuration checklists document desired security configuration settings, installed patches, and other system security elements in a standardized format. SCAP-enabled tools automatically generate assessment and compliance evidence, which is useful in computer forensics and other scenarios. SCAP measures and scores vulnerabilities within software, enabling quantitative and repeatable measurement and scoring.

Security practitioners should identify and obtain SCAP-expressed checklists relevant to their systems’ software, then customize the checklists as appropriate to meet specific organizational requirements. Customization is generally easy to do. After fully testing the checklists, organizations should implement their recommendations.

Organizations periodically need to verify the security of each system, which is much more difficult to do without standardized, automated checking tools. Further complicating system security management is the need to respond appropriately to new vulnerabilities and threats, prioritizing them so the most significant ones can be addressed sooner. Without enumerations, data correlation and product integration is mostly manual, unscalable, error prone, and costly. Data is locked in proprietary repositories.

Most enterprises use a variety of tools and applications to maintain and monitor their vulnerabilities. These tools identify security problems within applications, databases, systems, and networks. The lack of interoperability across sys-

tem security tools is another problem for security managers. For example, the use of proprietary names for vulnerabilities or platforms creates inconsistencies in reports from multiple tools, causing delays in security assessments and vulnerability remediation.

Security practitioners should encourage security software vendors to incorporate support for Common Vulnerabilities and Exposures (CVE), Common Configuration Enumeration (CCE), and Common Platform Enumeration (CPE) into their products, as well as encourage all software vendors to include CVE and CCE identifiers and CPE product names in their vulnerability and patch advisories.

SCAP is especially useful with managing all the vulnerability assessment scans that have generated tons of data, connecting this information, and understanding and prioritizing the issues when conducting remediation. Suppose the enterprise uses a variety of security tools, each generating overlapping bugs and false positives. In order to get these vulnerabilities closed, the security teams need to start sorting and moving this data around and getting the appropriate issues in front of management, developers, and engineers.

With SCAP, security teams have a common way to describe vulnerabilities. They can eliminate duplicates that reference the same common vulnerability on the same platforms. These vulnerabilities can be scored and prioritized for bug fixes. Management can view reports and metrics that showcase the vulnerability state across all applications, systems, networks, and databases. The time from identification of a security issue to remediation is drastically reduced with SCAP tools.

Security practitioners should use SCAP for quantitative and repeatable measurement and scoring of software flaw vulnerabilities across systems using a combination of the Common Vulnerability Scoring System (CVSS), CVE, and CPE. The ability to accurately and consistently convey the characteristics of vulnerabilities allows organizations to institute consistent and repeatable mitigation policies throughout the enterprise. CVSS base scores assist in prioritizing the remediation of known security-related software flaws based on the relative severity of the flaws. CVSS scores can be used more easily when using CVE to reference specific vulnerabilities. When a new vulnerability is publicly announced, a new CVE identifier is created for it, the affected products are identified using CPE, and the CVSS base measures and score are computed and added to the National Vulnerability Database,<sup>3</sup> the U.S. government repository of public vulnerability manage-

ment information. Organizations can review the CVSS base measures and scores for each new CVE as part of their vulnerability mitigation prioritization processes. SCAP content can be used to check their systems for the presence of the new vulnerability.

Oftentimes organizations must demonstrate that they have implemented security controls in accordance with some higher-level requirements, such as HIPAA, FISMA, SOX, etc. There are often varying levels of these controls, but SCAP can facilitate the traceability between the varying levels. This is needed when a security team must communicate their chosen security configuration and the rationale behind it. SCAP content can communicate security configurations to configuration, change, and asset management teams for integration in standardized builds and images. SCAP provides a comprehensive, standardized approach to overcoming these many challenges in IT security.

---

**With SCAP, security teams have a common way to describe vulnerabilities. They can eliminate duplicates that reference the same common vulnerability on the same platforms...and the time from identification of a security issue to remediation is drastically reduced.**

---

## Conclusion

In 2008, the National Vulnerability Database received 69,000,000 hits from entities like the Department of Homeland Security, the Payment Card Industry, and security products developers. Even more hits will occur as more and more commercial applications access it, and as more and more vulnerabilities arise. Without a standardized approach, enterprises will never get their head above water.

SCAP provides a transparent, interoperable, repeatable, and automated way to assess security software flaws and misconfiguration in the enterprise. Efficiencies gained through SCAP give IT security teams more time to address other issues. By linking compliance to configuration, SCAP makes compliance reporting a by-product of good security, allowing IT security teams to focus on securing the enterprise.

## About the Author

*Ken Halley, CISSP, is CEO of Gideon Technologies, developer of SecureFusion, which uses the Secure Content Automation Protocol to enable automated asset discovery, vulnerability and configuration management, and policy compliance evaluation in accordance with federal standards. Ken may be reached at [Khalley@gideontechnologies.com](mailto:Khalley@gideontechnologies.com)*



<sup>3</sup> <http://nvd.nist.gov/scapproducts.cfm>.