2010

BizTechReports

Enhancing Information Assurance with Security Content Automation Protocol

SignaCert Security Perspectives in the National CyberSecurity Arena

Enhancing Information Assurance with Security Content Automation Protocol

Introduction

The emergence of a national cyber security organization, with security responsibilities over both public and private sector IT infrastructure, creates significant new technical challenges for both the federal government and commercial organizations. In the coming years, government cyber security officials and CIOs of a wide variety of enterprises will be forging new relationships and developing innovative new processes to assure that IT infrastructure critical to American life are adequately protected from theft, subversion, espionage, or denial of service.

Already, the National Institute of Standards and Technology (NIST) have laid the groundwork for infrastructure that will allow the national cyber security organization to respond to vulnerabilities and threats to national IT infrastructure. NIST's Security Content Automation Protocol (SCAP, pronounced 's-cap') is an automated system designed to rapidly and broadly distribute security content—for example, malware or virus signatures, or information on known vulnerabilities—to the CIOs of a broad spectrum of infrastructure providing organizations.

SCAP, in turn, supplements a regime of certification and accreditation that assures, on a periodic basis, that IT infrastructure is adequately protected from known security threats. The periodic and static character of the certification and accreditation (C&A) auditing process, however, is increasingly recognized as a poor match for the current dynamic IT infrastructure environment: systems change with the introduction and evolution of software and hardware, while new threats emerge and old threats adapt and evolve at a pace much faster than the development of new C&A policies and practices.

“Under the traditional C&A model of enterprise IT security, CIOs and their staffs sign off on three-ring binders full of security practices and procedures,” explains Wyatt Starnes of leading IT security firm SignaCert. “Unfortunately, all that paper is obsolete as soon as it comes out of the printer,” says Starnes.

Inclusive vs. Exclusive Defense Models

In many ways, SCAP opens the door to add a much more proactive and aggressive dimension to the array of security measures enterprise IT professionals in both the public and private sector have pursued. Instead of simply looking to identify bad actors and code so that steps can be taken to keep them out of the environment through an exclusion strategy – which has been the underlying philosophy behind most anti-malware programs and strategies to date – SCAP provides the foundation for assertively maintaining a secure and compliant state at all times.

It allows for the creation of solutions that enable people, processes and technologies to be included in the system, as long as all elements touching the enterprise network conform with technical and operational models of behavior at multiple levels.

This is accomplished by integrating three critical areas of activity – Image Management, Configuration Management and Vulnerability Management – that typically have not been managed in a well coordinated manner in the past.

SCAP provides a way for security professionals to develop a proactive approach to security while also assuring continuous compliance with various institutional and government requirements and elevating the performance of key enterprise systems.

SCAP-enabled strategies start by creating a reference image model that carefully outlines exactly what systems – and sub-systems – should look like at a very granular level. It requires a very careful inventory of all the applications, drivers and services that run in any given environment within the enterprise. This abstracted reference model is then used to automate the process of constantly analyzing the production environment, and identify any new development that fails to match the model.

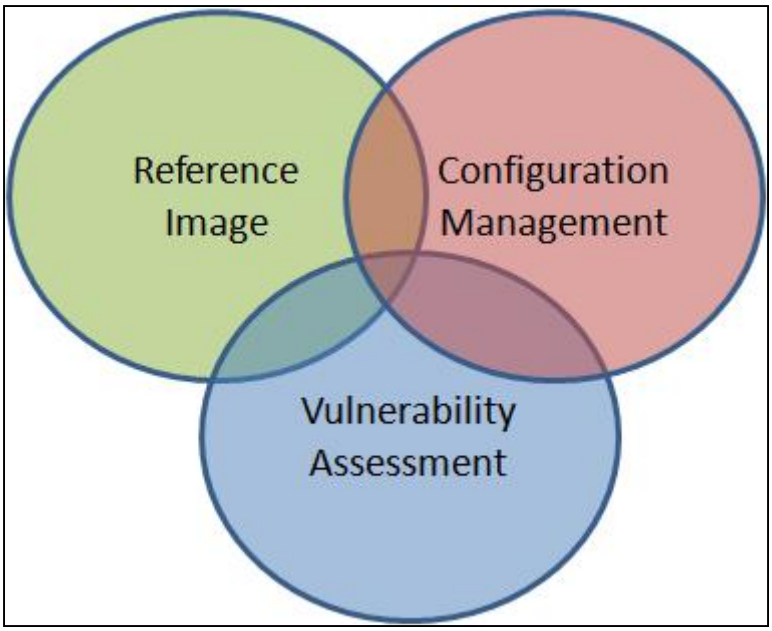

Figure 1 -- An Inclusive and Integrated Approach to Information Assurance

SCAP also allows organizations to develop effective configuration analysis paradigms so that security professionals can not only determine what is supposed to be in the environment, but also establish a very detailed understanding of how elements in the enterprise system are supposed to behave.

Finally, SCAP provides for a constant, automated assessment of vulnerabilities that may target hardware, software and configuration arrangements in the system by checking against libraries of potential configuration vulnerabilities that are used by the SCAP community. If vulnerabilities arise in the system, then the security and IT teams are immediately alerted. Working in the opposite direction, when new unpublished (zero-day) malware attacks, hack attempts or insider threats result in behaviors that create conflicts with any one of the multiple layers of reference models enabled by SCAP, an alarm will be immediately triggered. If, upon investigating an alert, the security team discovers a new threat – or uncovers a new vulnerability – then immediate steps can be taken to mitigate the threat. More importantly, however, the new threat and/or vulnerability is reported and published to a federated SCAP repository of threats and vulnerabilities. This has the immediate effect of inoculating the rest of the SCAP community.

"At the core of the model are all of the technologies and operating systems that run across all systems, and subsets to reflect any system differences," explains Starnes. For example, some Web servers might be built on an HP system, and other systems on an IBM system.

"In some cases, the operating system is the same, but the drivers are different. But it doesn't matter, because SCAP provides the tools that make it possible to take note of all those differences…and ensure that they are modeled separately. By modeling systems as they should be configured, SCAP-based solutions can detect any security issue on a comprehensive and continuous basis," he says.

Beyond Security

SignaCert, for instance, has developed a datacenter-ready implementation of the SCAP method that enables "continuous monitoring"

and affirmation of any IT platform regardless of vendor that are involved in the enterprise network. It leverages the SCAP protocols to enable standardized sharing of software integrity state, configuration and risk/vulnerability information.

Continuous monitoring with SignaCert's SCAP implementation dramatically enhances change detection resolution while closing the IT compliance exposure window.

With SignaCert Enterprise Trust Server version 3.6, customers can now operationally manage IT systems against SCAP vulnerability and configuration checklists (including FDCC). When assessing system security, vulnerability, and configuration posture, the Enterprise Trust Server utilizes information from XCCDF (Extensible Configuration Checklist Description Format), OVAL (Open Vulnerability Assessment Language), CVE (Common Vulnerability Enumeration), CCE (Common Configuration Enumeration), CPE (Common Platform Enumeration), and CVSS (Common Vulnerability Scoring System).

SignaCert has extended SCAP's traditional compliance-centric capabilities by providing robust reference image management validation supplemented by rich known-provenance whitelist content. This combination greatly enhances software supply chain confidence on all IT platforms, increasing the security and efficacy of managed systems.

"We see the SCAP method for Continuous Monitoring of IT systems used by DoD and the Federal IT community as a major step to enhance both security and operational compliance," says Starnes.

Conclusion:

The principal benefit of SCAP is that it provides for better assurance of operational readiness by moving IT infrastructure security from the old reactive and periodic C&A models of compliance toward a new process of continuous and automated monitoring. Effective SCAP-based strategies offer a way to proactively observe and respond to on-going threats, risks and vulnerability in real-time environments.

In an era when the most dangerous threats pose their greatest risks at the very minute they are introduced, anything short of a comprehensive, real-time, enterprise-wide solution leaves organizations exposed.

SCAP-based strategies will give CIOs and cyber security professionals a broader view into vulnerabilities and sensors, via active and automated comparisons against carefully designed reference models at multiple layers of technology as well as by interacting with threat libraries and resources that stay on top of malware and hacker trends.

This results in the ability to establish much more proactive change detection and system protection. It also improves availability and system uptime, while reducing operational expenses.

About SignaCert

SignaCert is the leading provider of end-to-end and partner-based IT compliance solutions based on known-provenance whitelist technology. These methods allow SignaCert's direct customers to rapidly achieve and prove continuous compliance for the systems that deliver critical business services. The SignaCert architecture is designed to seamlessly integrate with existing change processes and continuously monitor critical business services without disruption.

Additionally, SignaCert's OEM and ISV Partners can supply to, or license content from, the SignaCert Global Trust Repository (GTR), adding new and important capabilities to their product offerings. All use cases are supported by a rich repository of vendor-independent software measurements. These "white" or "allow" list methods enable SignaCert's patented technology to be quickly deployed and provide immediate visibility into the actual state of IT infrastructure.

Founded in 2004 by 34-year IT security and compliance industry veteran Wyatt Starnes, SignaCert has assembled a world class team of industry leaders with hands-on IT experience for its executive team, board of directors, and advisory board.

SignaCert's end-customers span a wide variety of industries, including financial services, government, and healthcare. For more information visit www.signacert.com

About BizTechReports.Com

BizTechReports.Com is an independent reporting agency with offices in Washington, DC and the San Francisco Bay Area that analyzes user trends in business technology. *BizTechReports.Com* explores the role that technology products and services play in the overall economy and/or in specific vertical industries. For more *BizTechReports.Com* white papers, case studies and research reports, visit www.biztechreports.com.

