



Improving Security Vulnerability and Configuration Management through a Service Oriented Architecture Approach

Overcoming the challenges to security vulnerability and compliance management through NIST standards and a Service Oriented Architecture (SOA) approach to streamline processes, improve security, achieve compliance and reduce costs.

Challenges of Federal Agencies

Security Threats Continue to Mount and Increase in Sophistication

Shawn Henry, the newly appointed Assistant Director of FBI's Cyber Division has warned that "a couple dozen" countries are eager to hack U.S. government, corporate and military networks. He withheld specific details of the countries in question but stated that cooperation with overseas law enforcements is of highest priority at FBI and that there has been great success fostering partnerships. However, Mr. Henry stated that certain countries have already mounted aggressive attacks against the U.S. particularly targeting websites under '.gov', '.mil', and '.com' top-level domains. "The threat that we face from organized groups that have infiltrated home computers, corporate computers, government computers [is] substantial and its impact on economy is a national security concern."

Organizations have worked to reduce vulnerabilities and adapted new technologies to detect and prevent security threats. However, attackers continue to create new and innovative ways to achieve their objectives. As a result, the threat landscape constantly shifts as the attackers identify weaknesses and exploit them through new more sophisticated techniques. Based on the data collected recently collected, analyzed and reported¹ by Symantec, we can observe that the current security threat landscape is predominantly characterized by the following:

- Malicious activity has become Web-based
- Attackers targeting end users instead of computers
- Underground economy consolidates and matures
- Rapid adaptability of attackers and attack activity

"As cyber criminals move beyond mass-distribution style phishing scams, they are learning how to localize and personalize their attacks for better penetration," according to the Georgia Tech Information Security Center (GTISC) report². Malware development expertise is rapidly maturing which provide the skills to exploit the continued weaknesses of poorly configured websites, applications and databases. As an example, the report described an exploit that sends a message from one person to another, about a YouTube video, including a link to the clip. The recipient clicks on the link, sees a prompt to download an updated version of Flash player to run the clip. When he clicks on the update, it actually installs malware on his computer.

Researchers at GTISC estimate that 15% of all online computers in 2008 will become part of botnets thereby being infected with code that puts these computers under the control of the botnet. Infections can occur even through legitimate Web sites as botnet delivery mechanisms are becoming more sophisticated. Users are unable to detect the threat and cannot deter it. Network managers can block known bad sites, but are unable to keep pace with the infections or cannot block access to a site for business reasons.

Another serious threat identified by GTISC is cyberwar. The report cites the evidence that implicates the Russian government in cyber attacks against Georgia. Cyber criminals are professional, organized and profit-driven, the report states. The report goes on to state that criminals now buy, lease, subscribe, or use a pay-as-you-go business model to obtain the latest in malware kits.



¹ <http://www.symantec.com/business/theme.jsp?themeid=threatreport>

² <http://www.gtiscsecuritysummit.com/pdf/CyberThreatsReport2009.pdf>

Applications and Databases Remain Vulnerable

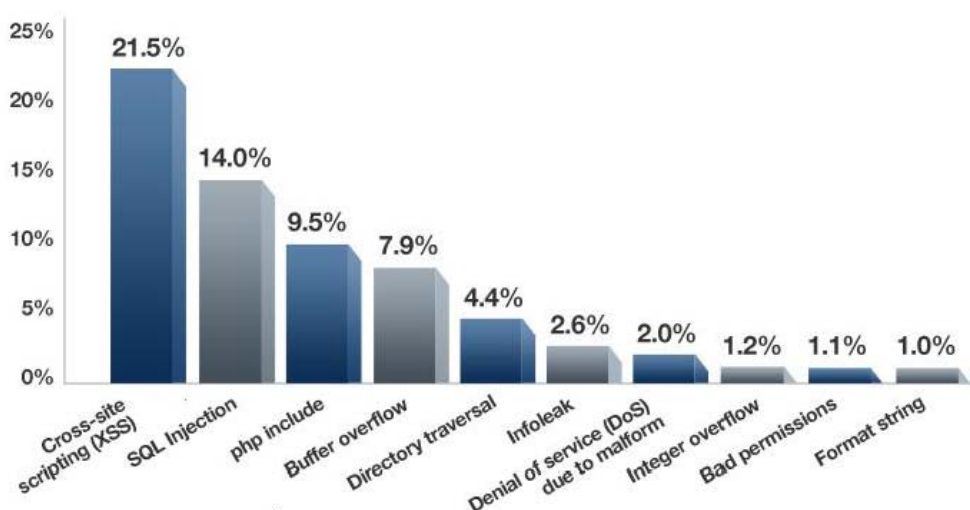
IBM's X-Force Lab reports³ that Web-based vulnerabilities and threats continue to increase. They found that:

- Over the past few years, the focus of endpoint exploitation has dramatically shifted from the operating system to the Web browser and multimedia applications.
- Vulnerabilities affecting Web server applications are climbing and so are the attacks, both evidenced by newcomers to the most vulnerable vendor list and this year's automated SQL injection attacks.
- Although standard Web browsers are becoming more secure, attackers continue to rely on automated toolkits, obfuscation, and the prevalence of unpatched browsers and plug-ins to successfully gain hold of new endpoint victims.
- Although the most exploited Web browser vulnerabilities are one to two years old, the availability of public proof-of-concept and exploit code is speeding the integration of more contemporary exploits into toolkits.
- In the first half of 2008, 94 percent of public exploits affecting Web browser related vulnerabilities were released on the same day as the disclosure.

For the second quarter of 2008, 7 of 10 Web applications used unsafe communication practices that could lead to exposure of sensitive information during transactions.

- Cenizic
- WhiteHat Security

IBM X-Force reports and Open Web Application Security Project⁴ (OWASP) confirms that the predominate types of vulnerabilities affecting Web applications are cross-site scripting (XSS), SQL injection, and file include vulnerabilities. The graphic below charts each type of vulnerability. In the past few years, cross-site scripting has been the predominant type of Web application vulnerability, but the first half of 2008 saw a marked rise in SQL injection disclosures, more than doubling the number of vulnerabilities seen on average over the same time period in 2007. This increase explains the spike in the percentage of Web application disclosures attributed to SQL injection.



Courtesy of OWASP

³ <http://www-935.ibm.com/services/us/iss/xforce/midyearreport/>

⁴ <http://www.owasp.org>

Security Policy and Regulations Continue to Mount with Increased Detail Required to Demonstrate Compliance

System and Software Configuration

The Federal Desktop Core Configuration (FDCC) is a standard security configuration mandated by the Office of Management and Budget (OMB). The FDCC currently exists for the Microsoft Windows XP Professional™ and Windows Vista Enterprise™ operating systems. In March 2007, OMB issued guidance to all federal agencies and departments requiring that they develop plans to adopt the standard security configurations by February 1, 2008. Agencies must determine if they can support their legacy applications and COTS software on these hardened configurations which eliminate administrator privileges, tighten security controls and restrict Internet Explorer functions. Additionally, agencies must report and manage any deviations from the standard as risks continuing to eliminate these risks through updating their legacy software or working with vendors to obtain new releases which operate on the FDCC platform. CIOs are required to continually scan agency computers to ensure security configurations are maintained in accordance with the FDCC standard.

FISMA and associated OMB guidance requires agencies to inventory all devices by operating system type, track the security configuration baseline applied to the device and then periodically test these devices for compliance. Annually agencies must report a summary of compliance for each system type.

Control Testing

Federal policy requires all systems to be certified and accredited (C&A). NIST has defined standards for C&A. To comply with C&A standards, a security plan must be developed and maintained which addresses implementation of security controls tailored to meet the needs of the system and the system security impact level (LOW, MODERATE or HIGH). NIST Special Publication 800-53 defines the security controls for Low, Moderate and High systems. There are over 160 security controls defined that span the following areas:



FAMILY	CLASS
Access Control	Technical
Awareness and Training	Operational
Audit and Accountability	Technical
Certification, Accreditation, and Security Assessments	Management
Configuration Management	Operational
Contingency Planning	Operational
Identification and Authentication	Technical
Incident Response	Operational
Maintenance	Operational
Media Protection	Operational
Physical and Environmental Protection	Operational
Planning	Management
Personnel Security	Operational
Risk Assessment	Management
System and Services Acquisition	Management
System and Communications Protection	Technical
System and Information Integrity	Operational

Until recently, system owners were free to determine the best way to assess the effectiveness of implementation of these controls as there was no standard. That allowed flexibility but also meant there was no standard. As witnessed by OIG assessments, many federal agencies did not assess controls to what the OIG would describe as satisfactory.

NIST has now published NIST SP 800-53A. This standard defines the assessment cases required for each of the 160+ security controls. In most instances, there are more than 5 assessments per control. Organizations that do not organize to optimize control implementation and assessment efforts will face major increases in costs to annually maintain the C&A of its systems. NIST SP 800-37 also requires controls to be assessed at least annually (more frequently for HIGH system). Therefore, automation to the greatest extent possible combined with making sure an organization and leverage all testing and assessment efforts performed throughout the year by different parts of the organization will help to drive down costs, reduce security risks, and increase compliance.

To gain a sense of impact of the requirement to follow NIST SP 800-53A, previous efforts were not found to test the 160 controls effectively. The new standard raises the bar by defining an average of over 800 assessments to test the same 160 controls.

Independent Testing

Organizations provide software solutions through a variety of means. Some organizations have the expertise in house and use this to develop and maintain software. For the organizations that lack this expertise or have chosen to outsource this capability, software is developed under contract. Frequently, this software is not tested for security vulnerabilities prior to be deployed to production.

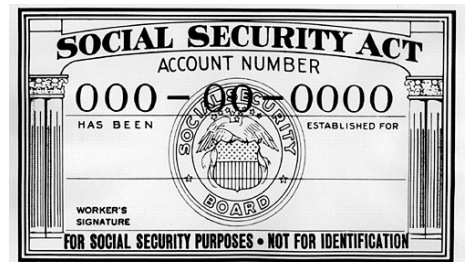
Most organizations augment custom developed applications with a variety of commercial off the shelf software (COTS), government off the shelf software (GOTS) and may also have moved to incorporating open source into their software baseline.

If software supports a system categorized as a MODERATE or HIGH system by FIPS PUB 199 or is part of a system that is on the agencies Critical Infrastructure Protection (CIP) inventory, then NIST requires the system control testing to be performed by an independent party (CA-4 and CA-7).

Inventory, Protection and Tracking of Sensitive Information

The Office of Management and Budget issued memo [M-06-16 "Protection of Sensitive Agency Information"](#) which provided additional guidance to agencies regarding protection of Personally Identifiable Information (PII). This memo required all federal agencies to:

- Encrypt all data on mobile computers/devices which carry agency data unless the data is determined to be non-sensitive. This spans PDAs, laptops, USB storage devices, and backup media;
- Allow remote access only with two-factor authentication where one of the factors is provided by a device separate from the computer gaining access;
- Use a "time-out" function for remote access and mobile devices requiring user re-authentication after 30 minutes inactivity; and
- Log all computer-readable data extracts from databases holding sensitive information and verify each extract including sensitive data has been erased within 90 days or its use is still required.



Many agencies have had success in implementing the first three recommendations from OMB. However, the fourth recommendation has been significantly more challenging.

Security Risks Inherent in 3rd Party Software

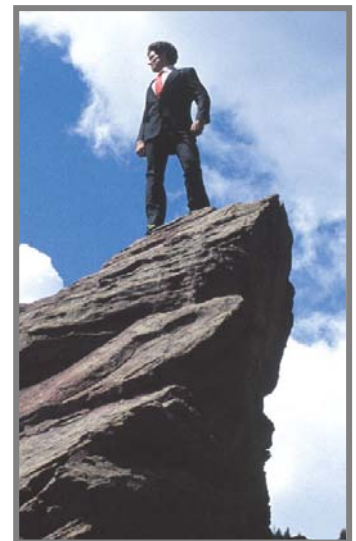
Organizations face a daunting challenge in trying to understand and control security risks across their varied software supply chain. Agencies rely on third-party software and service providers to provide mission critical software to support their agencies. The burden of minimizing risk from third-party software falls on the organization head that acquires the software or that own the system. However, these risks cascade throughout the total connected enterprise and its partners. OMB has begun to address this through requiring future purchases of software to be compliant with FDCC. However, this only addresses desktop applications and does not address enterprise software or software installed on servers. Additionally, compliance with FDCC only confirms configuration and does not ensure that software does not contain vulnerabilities or malware. Agencies need a way to evaluate software for security risks prior to acquisition or to include the requirement to undergo testing as a condition of acquisition. Further, as custom software is changed or new releases of commercial 3rd party software are made available, agencies need a solution to evaluate the new release of software prior to deployment.



Need to Improve Security Management and Situational Awareness

Federal government Chief Information Officers (CIO) and Chief Information Security Officers (CISOs) are charged with increased responsibility for protecting information. They face a daunting task frequently complicated by siloed security management, monitoring, measurement, and auditing environments. Threats are increasingly complex and more targeted which further increases the burden on IT operations. Adding to these burdens and complexity is the fact that the President, Congress and OMB are rapidly enacting new laws and policies that require agencies to implement additional security safeguards, assert more control, and provide detailed metrics to measure performance and demonstrate compliance. Often times, these additional security safeguards and the associated reporting are not funded.

CIOs and CISO are confronted with organizational, technical and financial barriers when it comes to security management and security situational awareness. For large organizations, there is frequently an abundance of tools. Often times, these tools are limited in capability, and are not standardized across the agency. Generally, these tools store information in proprietary formats and are not designed to fit into the overall security information management architecture. Many times, the budget for security is spread across the agencies systems which, if effectively planned and implemented can deliver the security required of the system. But frequently this is at a cost to overall security management and situational awareness and often time increases cost due to redundancy or lack of economies of scale.



Overcome these Challenges

Protecting sensitive information and digital assets is a complex challenge. Unfortunately, the threats to this information and assets continues to grow, are becoming more targeted and sophisticated. At the same time, Agencies are under constant pressure to deliver services more rapidly over a wider array of networks,

devices and boundaries. The combination of increasing threats and vulnerabilities together with the demand for ubiquitous access to information and services increases the risk of security breaches and exposures.

CIOs must take stock of their agency's existing security architecture, security tools and services and develop a road map which addresses required capabilities leveraging existing investments and incorporating shared services and approved tools where applicable. Solutions must be extensible and permit integration and correlation of data from many sources.

Our approach and solutions address the information security challenges faced by many agencies and can be adapted to the unique needs of your agency. We tailor our approach and solutions based on your organizational structure, the data your organization processes and the current level of maturity of your information security program.

Do More With Less

In today's challenging economic environment, organizations need to cut costs while providing a higher level of service. The SecureIT solution of automation, on-demand delivery and integrated technology enables organizations to address mounting security threats without adding full time resources. Through a web-services model, our integrated technology solution leverages existing software where it is cost effective. In many instances, organizations can reduce the security software products used through an enterprise approach. Additionally, the solution enables your organization to identify opportunities to reduce or manage costs for installed COTS software product licenses. SecureIT enables organizations to improve the productivity of their existing resources and security investments through standards and automation.



Improve Vulnerability Detection and Speed Remediation

Vulnerabilities exist at every level of your IT infrastructure. Frequently, organization focus solely at the network and device level which leaves applications and databases untested. In many cases, vulnerability assessment is performed in differing levels and frequency which commonly result in gaps leaving assets untested, inadequate testing and no management of the information. Our solutions address the individual needs of each layer of vulnerability assessment and provide an integrated solution that achieves vulnerability management, optimizes resources, and eliminates gaps in security management.

Platform Security Configuration Compliance to ensure your network assets are configured to meet your security policy as well as national standards. The Federal Desktop Core Configuration (FDCC) is required for all agencies. Additionally, the NIST Checklist program has established security configuration standards for most operating system platforms and some database management systems. Our solution provides the means to assess assets to determine if they are configured to comply with your organization's policies and national standards. Reports identify non-compliance along with associated vulnerability and remediation. The solution can continuously test or audit the configuration of your IT assets to provide deep insight into critical asset management and security management. The solution can be deployed at a component level and feed an enterprise system or can be deployed at the enterprise level and import data from components to provide an enterprise-wide report.

- *Achieve immediate results without operational impact*
- *Easily prepare reports in required format by OMB*
- *Monitor progress on remediation*
- *Monitor software license usage to pay only for licenses used*
- *Verify patches are deployed*
- *Reduce time and cost associated with evidence to support audits*
- *Demonstrate compliance and improve FISMA performance*
- *Meet NIST SP 800-53 requirements for HIGH systems through automated process to maintain an up-to-date, complete, accurate, and readily available baseline configuration of the information system (CM-2)*

Network Vulnerability Assessment using Nessus™ or your currently installed network vulnerability scanning software⁵, to identify vulnerabilities and lack of patches in network assets. The solution scans for thousands of known vulnerabilities in servers, workstations, network devices, and applications. When deployed as an application, continuous scanning, detection, correlation and reporting can be achieved. Vulnerability signatures are updated on a daily basis and provide checks for the most recent security vulnerabilities reported to the NIST National Vulnerability Database (NVD).

- *Use of leading industry recognized Nessus scanner or your currently installed vulnerability scanner software which is NIST validated*
- *Agent-less vulnerability, patch, content and configuration auditing*
- *High speed vulnerability identification on the assets selected*
- *Supports distributing scanners throughout the enterprise to optimize for network or for organizational control and responsibility*

Application Vulnerability Assessment through either dynamic testing or static binary code analysis to assess attack resistance and discover application vulnerabilities. Through this combined approach, we can analyze both web and non-web applications to detect flaws in the software inputs and outputs which detect vulnerabilities introduced by linked libraries, APIs, compiler optimizations, open source software and other third party components.

- *The most accurate and complete application security testing available.*
- *Security weaknesses with the severity as well as areas of non-compliance with applicable security policy (e.g. FISMA) and security standards (e.g., NIST).*
- *Actionable information to remediate the weaknesses, correct non-compliance or implement process improvements.*
- *Static binary analysis supports applications written in C/C++ on Solaris, Windows and Linux; C# on Windows as well as any Java (J2EE, J2SE and JSP) applications.*
- *Dynamic analysis (web scanning) supports any web application built using common web languages without client side computing (e.g. AJAX, Flash, ActiveX).*
- *Shift the responsibility and operational cost of application security from your organization to the providers*
- *Quantify unbounded risk associated with third-party software*
- *Establish thresholds for purchased software, before it is deployed*



Database Vulnerability Assessment to evaluate the security strength of your database environments and compare them with national security best practices. Our

⁵ Must be compatible and validated by NIST for Authenticated Vulnerability and Patch Scanner

solution examines the patch levels, the software installed, and the configuration of the database to highlight vulnerabilities that may exist in the database environment. We provide a report with a set of recommendations as to what is required in order to remediate the problems.

- *Lightweight agent installed on each database server to determine aspects that cannot be determined remotely*
- *Passive network monitoring to discover vulnerabilities and dangerous behavior by observing database transactions at the network level*
- *Scanning to assess vulnerabilities such as mis-configured account controls and insecure passwords by interrogating the database server over the network through credentialed access*
- *Evaluate compliance against best practices library of vulnerability and configuration tests, based on NIST, DOD and NSA standards*
- *Generate a security health report card with weighted metrics (based on best practices) and recommends concrete action plans to strengthen database security*
- *Supports Oracle, SQL Server, DB2 (Linux, Unix, Windows), Informix, Sybase and MySQL*
- *If deployed as a solution:*
 - *Granular, real-time policies to prevent unauthorized or suspicious actions by privileged database accounts or attacks from unauthorized users*
 - *Perform continuous monitoring of applicable NIST SP 800-53 security controls to comply with certification and accreditation and FISMA*
 - *OMB 06-16: Log all data extracts from databases holding sensitive information*
 - *OMB 06-16: Provide data owner reports on data extracts and provide workflow process and tracking to validate continued need or certify data is erased within 90 days or its use.*

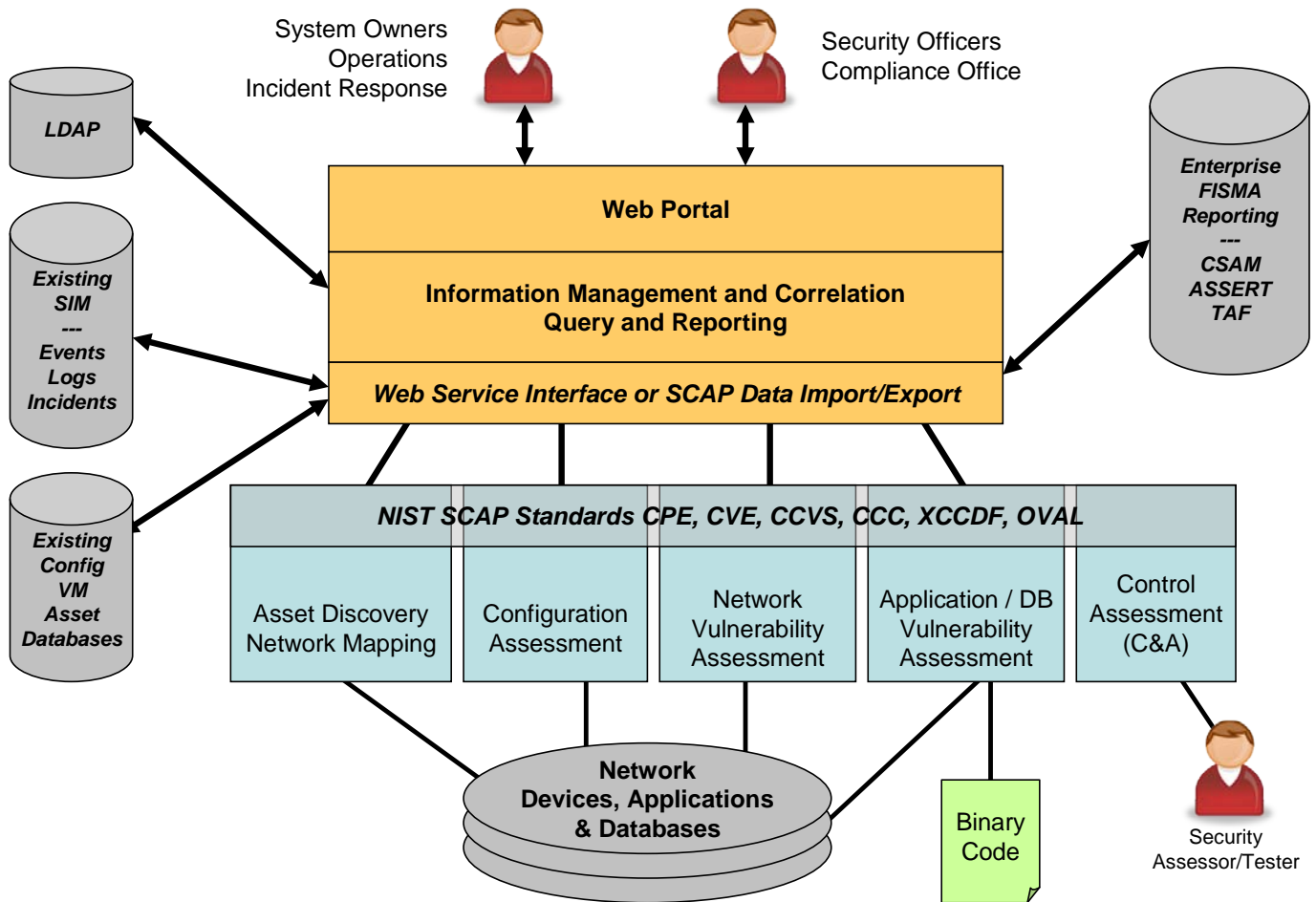
NIST recently published a [Frequently Asked Questions \(FAQ\) for Sensitive Data Extracts](#)⁶. In this FAQ NIST answers common questions regarding OMB Memo 06-16. It provides guidance on the data which must be audited, the information that needs to be contained in the audit log, and provides approved methods for verifying that extracted data is either still required or has been deleted. Our solution addresses these requirements to enable your organization to rapidly identify the sensitive data, monitor and log the extractions and provide a web-based means to manage continued need or verification of deletion.

Manage Information to Achieve Situation Awareness and Compliance

The NIST Information Security Automation Program (ISAP) is a U.S. government initiative to foster the development and adoption of standards to further the automation and standardization of technical security operations. The Security Content Automation Protocol (SCAP⁷) is a method for using specific standards to enable automated vulnerability management, measurement, and policy compliance evaluation. SCAP provides standards and promotes the development of tools that integrate and correlate data for asset, configuration, vulnerability and compliance management. SCAP sets the stage for automation and enables interoperability and repeatability as interim value.

⁶ csrc.nist.gov/drivers/documents/OMB/OMB-M-07-16-Data-Extract-FAQ.pdf

⁷ <http://nvd.nist.gov/scap.cfm>



Service Oriented Architecture (SOA) Approach with Web Services for Integrated Asset, Configuration and Vulnerability Assessment and Management

Agencies have an unprecedented opportunity to move from discrete, disconnected, point security management and monitoring solutions to a holistic, integrated strategy. Agencies can identify, classify and protect sensitive information within a security information management architecture. Our approach leverages commercially available technology and standards such as SCAP, Service Oriented Architecture (SOA) and Web Services to deliver significant cost savings and improved security management, situational awareness, performance measurement and compliance with FISMA and other security laws and policies.

Using a Service Oriented Architecture (SOA) model and Web Services to enables your organization to incorporate and access asset, configuration and vulnerability information from other repositories and tools on your network. Using this approach, your organization can leverage your installed base of assessment tools while establishing repeatable, automated scanning processes across your enterprise.

This approach integrates the results from many activities and correlates the information to avoid gaps and redundant efforts. It provides historical results,

remediation tracking and other vulnerability and compliance management functions for effective benchmarking, trending, metrics and reporting.

- *Provide automation and workflow from detection to remediation validation.*
- *Consolidated system patch reporting by vendor and by vendor bulletin to identify gaps and trends in your system patch processes.*
- *Filter results to exclude compensating controls and false positives to increase efficiency*
- *Leverage a Service Oriented Architecture (SOA) to scale from single agency to enterprise department and enable central management and distributed across the enterprise to optimize scanning and minimize network impact.*
- *We-based reporting system that allows custom reporting*
- *View, prioritize and monitor remediation*
- *Integrate with existing Security Information Management (SIM) solutions as well as existing asset, configuration and vulnerability assessment and management solutions through either Web Services or data import following SCAP standards*
- *Integrate with existing help desk, change management, incident reporting and trouble ticketing systems to ensure appropriate notification, tracking, and action*

About SecureIT

SecureIT helps private and public sector clients manage technology risks and create value through effective practices in IT security. SecureIT provides services and solutions in the areas of Cybersecurity, Information Assurance, Governance & Compliance, IT Audit, and Security Training. SecureIT designs enterprise security programs, implements best practices and assesses technology implementation for security risk. Professionals with industry knowledge and technical expertise devise strategies and solutions to reduce risk, increase efficiency and overcome the challenges of compliance. Located in Reston, VA, SecureIT serves clients in the Federal government including; DISA, HHS, DOJ, Treasury, Commerce, USAID, Education, DHS, and IMF as well as the private sector with clients such as Freddie Mac, CSC, FINRA, and E*TRADE.

For more information, call 703.464.7010, email info@secureit.com or visit www.secureit.com

Notice

The SecureIT logo, and all page headers, footers and icons are trademarks or registered trademarks of SecureIT Consulting Group. Other company names or products mentioned are or may be trademarks of their respective owners. Information in this document is subject to change without notice.