Data Sheet: IT Compliance

Symantec Risk Automation Suite

An SCAP-validated solution

Symantec Risk Automation Suite (formerly SecureFusion) capabilities relate directly to the objectives of the National Institute of Standards and Technology (NIST) Secure Content Automation Protocol (SCAP), a method for using specific standards to enable automated and integrated vulnerability management, measurement and policy compliance evaluation. Symantec Risk Automation Suite is the leading fully SCAP-validated enterprise class solution that provides accurate, continuous and automated IT risk metrics.

Providing a clear view of IT risk in accordance with SCAP

The Symantec Risk Automation Suite helps organizations continuously discover and visualize all IT networks and assets, prioritize risk accordingly and measure remediation efforts for the most complete, accurate, repeatable risk assessment of the IT environment. Risk Automation Suite has received the following SCAP validations from NIST:

- Federal Desktop Core Configuration (FDCC) Scanner – able to audit and assess target systems for FDCC compliance and reporting; has options included for agent-less, dissolving-agent, or persistent-agent scanning
- Authenticated Configuration Scanner – able to audit and assess target systems for compliance with defined configuration requirements
- Authenticated Vulnerability and Patch Scanner – able to scan target systems to locate and identify software flaws and evaluate patch status and compliance with patch policy
- Common Configuration Enumeration (CCE)
- Common Vulnerability Scoring System (CVSS)

Risk Automation Suite automatically measures IT security and compliance for standards such as the following:

- Federal Information Security Management Act (FISMA)
- Federal Desktop Core Configuration (FDCC)
- Certification and Accreditation (C&A)
- NIST 800 Series (NIST 800-53r3)
- Health Insurance Portability and Accountability Act (HIPAA)

Symantec Risk Automation Suite

The Risk Automation Suite includes four critical modules:

- **Asset Discovery—**rapidly discovers and inventories all networks and assets, including managed and unmanaged devices, and enables network leak detection.
- **Vulnerability Management—**conducts ongoing vulnerability detection and reporting for operating systems, infrastructure, network applications and databases.
- **Configuration Management—**maintains an accurate inventory of system configurations, including installed software, user accounts and system changes.
- **Policy Management—**continuously evaluates system configuration and compliance with standards and policies.

Symantec Risk Automation Suite Management Framework for SCAP

All four modules continuously provide information into a centralized Risk Automation Suite portal, enabling a streamlined, end-to-end measurement process—from asset discovery to analytics, reporting, and workflow. With SCAP-validated vulnerability and configuration scanning options included for agent-less, dissolving-agents, and persistent-agent operation, Risk Automation Suite helps public sector agencies measure and verify compliance with FISMA, FDCC, C&A, NIST, and HIPAA standards within hours of installation. Users also have an option for scanning off-network devices, with results imported into the portal if required. The portal provides an overall IT risk management framework for collecting, reporting and managing compliance and security information; and it is the central point of integration and automation between modules and other IT systems, providing a holistic view of the entire IT environment, as well as the workflow and reporting functions necessary to support compliance programs.

Asset Discovery for SCAP

Knowing your network, and what assets are connected to the network is essential to identify, prioritize and mitigate security risks. The Asset Discovery module performs a continuous network-based network and asset inventory via a high-speed unauthenticated agent-less network scans, delivering the data to the Risk Automation Suite portal for automatic asset classification, categorization and alignment with the agency’s critical systems to support the C&A process. Analytics within the portal identify rogue networks and hosts, and enable quick network leak detection and mitigation.

Vulnerability Management for SCAP

The Vulnerability Management module controls the scans for thousands of known vulnerabilities in operating systems, infrastructure, network applications and databases. The module offers management and workflow capabilities to speed and automate the entire vulnerability management lifecycle, and provides options for authenticated SCAP vulnerability scans that reduce the known issues of false-positive and false-negatives, and can leverage existing commercial or open-source un-authenticated vulnerability scanners. The portal collects all vulnerability data, automatically prioritizes findings, and provides detailed reporting by agency unit, platform, network, asset class and vulnerability type. Symantec Risk Automation Suite Vulnerability Management is compliant with the Common Vulnerabilities and Exposures (CVE) requirements and the National Vulnerability Database (NVD) initiative, and leverages our own library of SCAP developed content, as well as public SCAP vulnerability checking repositories such hosted by RedHat and MITRE.

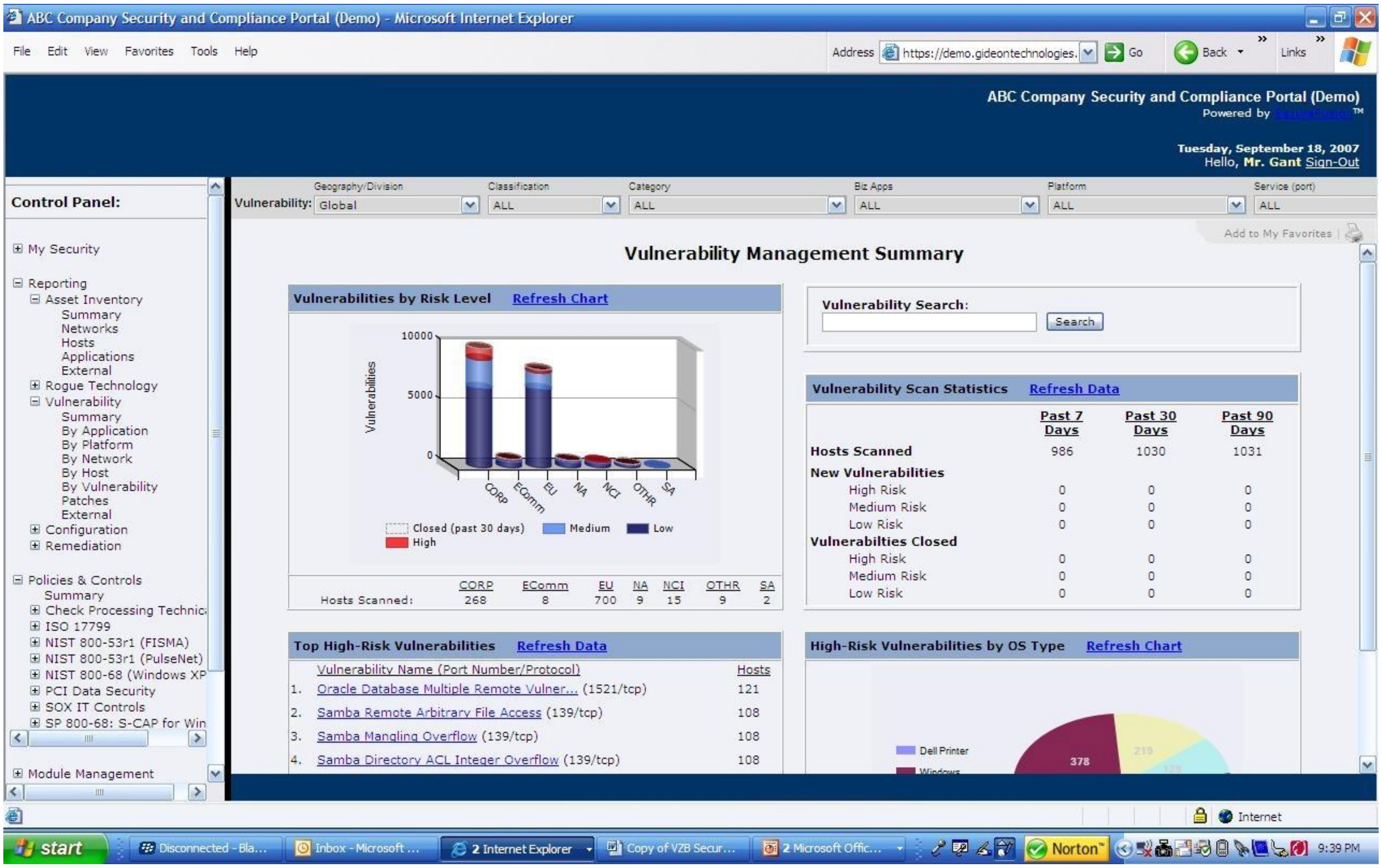
Configuration Management for SCAP

The Configuration Management module continuously captures the status of technical controls across the IT environment, including installed software, file sharing, user access, system patches and end-user controlled security settings. The module employs a lightweight process that helps gather critical compliance information without impacting IT operations or making changes to existing systems. Configuration Management includes several hundred of the most common asset configuration IT control checks out of the box, and can be configured to capture more based on the specific needs of the organization. In accordance with SCAP, Configuration Management is compliant and validated with the following requirements:

- Extensible Configuration Checklist Description Format (XCCDF)
- Common Platform Enumeration (CPE)
- Common Configuration Enumeration (CCE)
- Additional original equipment manufacturer (OEM) and NIST SCAP checklists

Policy Management for SCAP

The Policy Management module automatically measures and monitors compliance with IT control requirements in an SCAP-validated manner. Use the module to import NIST or industry SCAP-compliant checklists for immediate application in the appropriate environments, and to address specific requirements. Continuous reporting is one of the foremost benefits of the Symantec Risk Automation Suite. The portal communicates data from each module throughout the entire process using a variety of formats designed for specific roles within the IT department and the organization.



ABC Company Security and Compliance Portal (Demo) - Microsoft Internet Explorer

File Edit View Favorites Tools Help
Address https://demo.gideontechnologies.
Go
Back
Links

ABC Company Security and Compliance Portal (Demo)
Powered by

Tuesday, September 18, 2007
Hello, **Mr. Gant** Sign-Out

Control Panel:

- My Security
- Reporting
  - Asset Inventory
    - Summary
    - Networks
    - Hosts
    - Applications
    - External
  - Rogue Technology
  - Vulnerability
    - Summary
    - By Application
    - By Platform
    - By Network
    - By Host
    - By Vulnerability
    - Patches
    - External
  - Configuration
  - Remediation
- Policies & Controls
  - Summary
  - Check Processing Technic
  - ISO 17799
  - NIST 800-53r1 (FISMA)
  - NIST 800-53r1 (PulseNet)
  - NIST 800-68 (Windows XP
  - PCI Data Security
  - SOX IT Controls
  - SP 800-68: S-CAP for Win
- Module Management

Vulnerability: Geography/Division: Global; Classification: ALL; Category: ALL; Biz Apps: ALL; Platform: ALL; Service (port): ALL

Add to My Favorites

Vulnerability Management Summary

Vulnerabilities by Risk Level Refresh Chart

	CORP	EComm	EU	NA	NCI	OTHR	SA
Hosts Scanned:	268	8	700	9	15	9	2

Vulnerability Search: Search

Vulnerability Scan Statistics Refresh Data

	Past 7 Days	Past 30 Days	Past 90 Days
Hosts Scanned	986	1030	1031
New Vulnerabilities			
High Risk	0	0	0
Medium Risk	0	0	0
Low Risk	0	0	0
Vulnerabilties Closed			
High Risk	0	0	0
Medium Risk	0	0	0
Low Risk	0	0	0

Top High-Risk Vulnerabilities Refresh Data

	Vulnerability Name (Port Number/Protocol)	Hosts
1.	Oracle Database Multiple Remote Vulner... (1521/tcp)	121
2.	Samba Remote Arbitrary File Access (139/tcp)	108
3.	Samba Mangling Overflow (139/tcp)	108
4.	Samba Directory ACL Integer Overflow (139/tcp)	108

High-Risk Vulnerabilities by OS Type Refresh Chart

Symantec Risk Automation Suite benefits

Symantec Risk Automation Suite puts IT risk and security information at the fingertips of those who require it—whether the security administrator or an executive. Navigating between summary reporting and executive dashboards to specific, descriptive and granular reports is just a click away in the portal.

- Visualize the IT environment in less than a day with Risk Automation Suite Network and Asset Discovery. Use the portal to view a summary of all networks and with one click, see the entire inventory of network attached devices and hosts (even when they are not part of a known domain).
- Prioritize IT risk by going from vulnerability and configuration overviews to viewing the information by network, business unit and/or policy. Access the specific systems to manage the remediation process or document for audit purposes.

- Measure and report on IT risk and remediation by viewing continuous summaries against policy compliance imported directly in accordance with SCAP guidelines. View each technical control being measured, each asset's compliance and critical context regarding the asset.

More information

Visit our website

http://go.symantec.com/federalgovernment

http://www.gideontechnologies.com/federal_solutions.asp

To speak with a Product Specialist in the U.S.

Call 1 (703) 668-8945

About Symantec

Symantec is a global leader in providing security, storage and systems management solutions to help consumers and organizations secure and manage their information-driven world. Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored.

Symantec Public Sector Headquarters

2350 Corporate Park Drive, Suite 300
Herndon, VA 20171 USA
http://go.symantec.com/federalgovernment

Symantec helps organizations secure and manage their information-driven world with high availability, and disaster recovery solutions.