Automated STIG & CIS Compliance Assessment for IT Auditors

An EiQ Networks White Paper

Overview

Today, IT Security Auditors face a unique challenge: quickly determining the compliance of an IT system with predefined regulations in little time with few resources. Unfortunately, many compliance tools available to help with this task are not designed for auditors. They are designed for an organization responsible for the operation and continued monitoring of an IT system. Such tools do not help auditors because they must be “deployed” in order to use them. They are not designed to allow an auditor to quickly conduct an assessment and then leave for the next assignment.

As a result, auditors are left with few tools and mainly manual processes to properly assess an environment for compliance against the DISA STIGs or CIS policies. Such manual processes are prone to errors, require the physical presence of a team, and can be extremely labor-intensive.

To address these unique auditor needs, EiQ Networks has developed the SecureVue® Auditor License. This solution allows an IT Security Auditor to collect configuration data from a wide range of network devices and hosts, and compare the configurations to the secure standards defined by DISA. SecureVue then generates a detailed report that shows compliance violations by severity for each rule. The solution saves time and increases accuracy by automating the data collection, analysis, and compliance reporting.

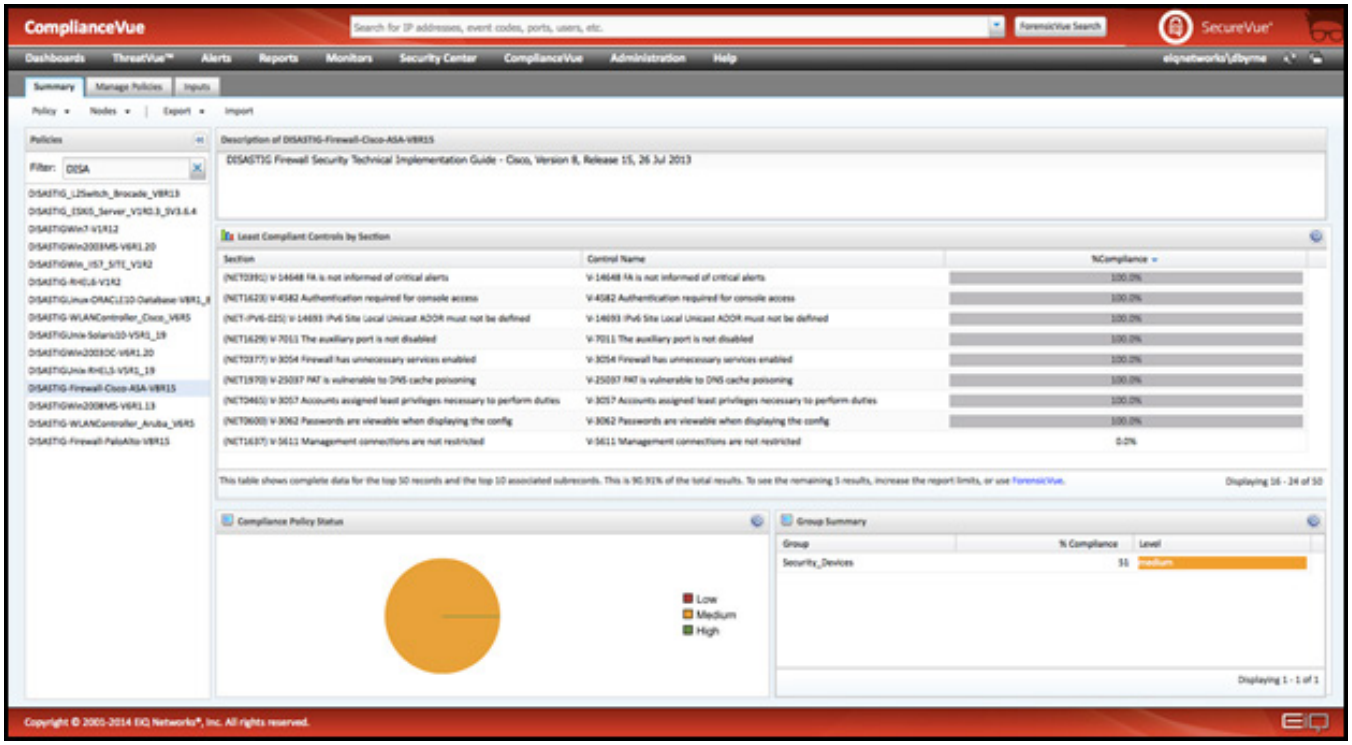
Configuration Auditing with SecureVue

SecureVue Auditor License transforms SecureVue from a continuous monitoring platform into a portable solution for auditors on the go.

SecureVue combines log management, SIEM, and configuration auditing capabilities in a single solution. SecureVue’s ComplianceVue® technology provides configuration auditing for workstations, servers, and network devices without the need to install an agent on individual devices.

Configuration data can be audited against:

- Defense Information Systems Agency (DISA) STIGs
- Center for Internet Security (CIS) Benchmarks
- User-created compliance policies
- User-selected reference nodes



SecureVue greatly simplifies the process of collecting device settings, comparing them to the mandated settings, and reporting on compliance violations. Each of these steps is fully automated in SecureVue. EiQ also maintains a built-in library of DISA STIG and CIS compliance policies that automate far more technical checks than SCAP and similar tools.

With the launch of the SecureVue Auditor License edition, these great configuration auditing features are now available as a portable solution for traveling IT Security Auditors. Unlike traditional compliance monitoring tools, SecureVue Auditor License is designed to be carried on a laptop and features easy setup when visiting a new audit location.

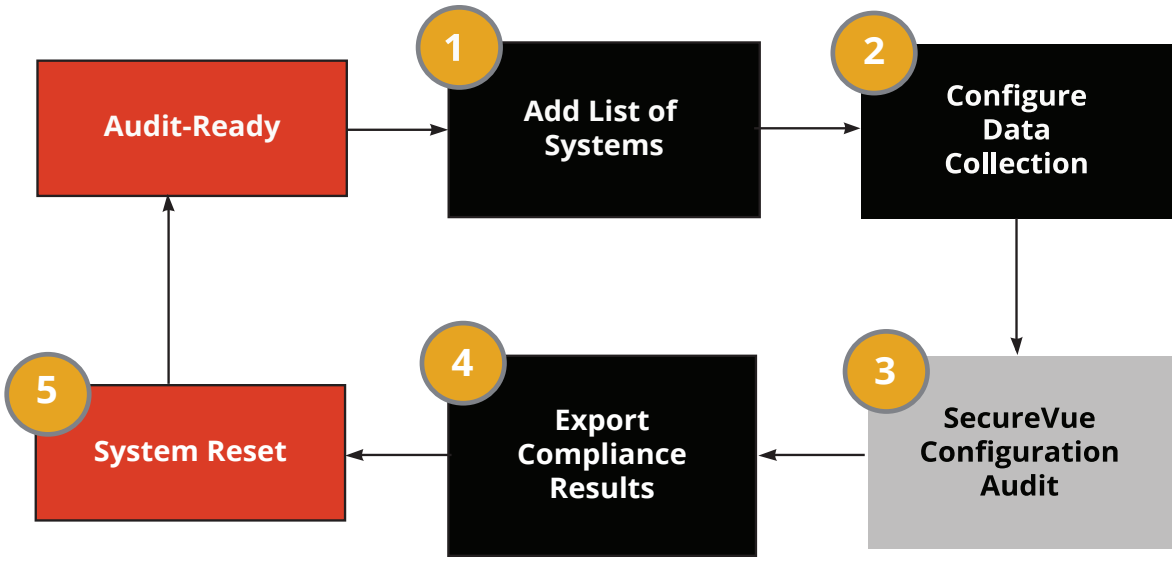
How It Works

The SecureVue Auditor License is a self-contained virtual server that can be installed on a laptop with VMware Workstation. This makes it simple to install and operate.

Once the application is installed, an IT Security Auditor can be ready to check devices against STIG compliance in two easy steps:

1. Import a .csv file of networked systems and the corresponding operating system information into SecureVue. This file can easily be created using the EiQ STIG Profiler or other network discovery tool.

2. Configure the access credentials for each system group (Windows 2003 Servers, RHEL Servers, etc.). As a clientless solution, SecureVue leverages protocols such as SSH and WMI to collect configuration data from your networked systems. Access credentials can be set for an entire group or individually for systems that don't share the same service accounts.



3. Once the first two steps are completed, SecureVue will automatically begin collecting configuration data from each system and audit against DISA STIG and CIS compliance policies.

4. After the SecureVue audit completes, export the compliance results using SecureVue's reporting templates (Include sample of report).

5. Reset the SecureVue virtual server to remove the data and return to an Audit-Ready state.

There is no need to set up individual systems for collection and no manual compliance auditing. These steps are fully automated by SecureVue. You can add further automation by using the EiQ STIG Profiler for device discovery.

Supported STIGs

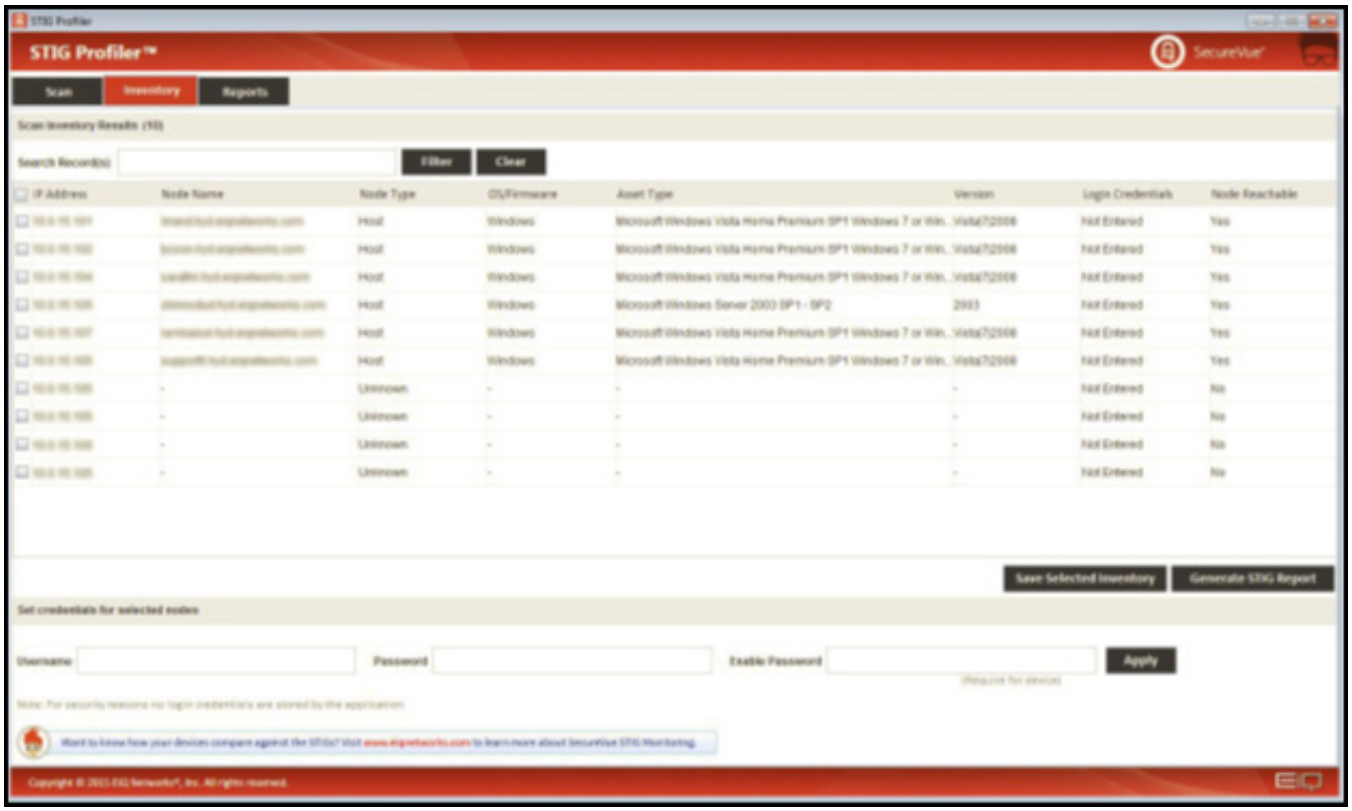
EiQ maintains a library of DISA STIG compliance policies that allow SecureVue to automate the data collection and compliance checks for the most common operating systems, network devices, and applications.

Sample DISA STIG Policies for SecureVue	
Aruba WLAN Controller	Microsoft IIS 7
AIX 6.1	Microsoft Office 2010
Brocade L2 Switch	Microsoft Office 2013
Checkpoint Firewall	Microsoft SQL Server 2000
Cisco ASA Firewall	Microsoft SQL Server 2005
Cisco IPS/IDS	Oracle Database 9
Cisco Network Infrastructure Router	Oracle Database 10
Cisco Network Perimeter Router	Oracle Database 11
Cisco L3 Switch – Perimeter	Palo Alto Firewall
Cisco L3 Switch – Infrastructure	Red Hat Enterprise Linux 5
Cisco IOS L2 Switch	Red Hat Enterprise Linux 6
Cisco Nexus L2 Switch	Solaris 10
Cisco WLAN Controller	SUSE Linux 11
Exchange Server 2010	VMware ESXi VCenter & Server 5.x
Foundry L2 Switch	VMware ESXi Virtual Machine
HBSS ePO	Windows 7
Internet Explorer 8	Windows Server 2003
Internet Explorer 9	Windows Server 2008
Juniper Network Perimeter Router	Windows Server 2008 R2
Juniper Network Infrastructure Router	Windows Server 2012

EiQ makes frequent updates to the built-in STIG library, and adds new content based on user requests.

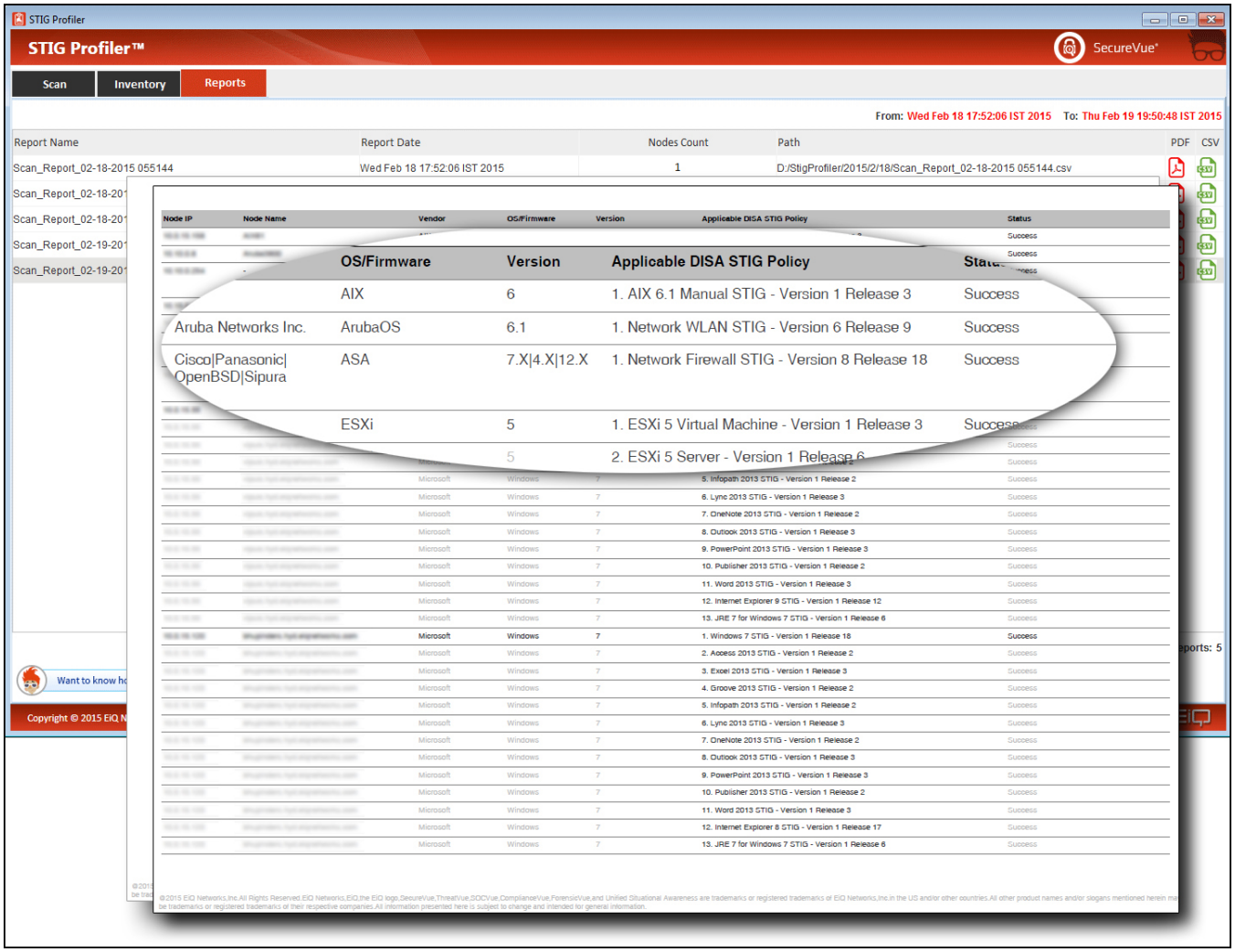
STIG Profiler Free Tool

As a supplement, EIQ Networks also offers the SecureVue STIG Profiler. The SecureVue STIG Profiler is a free software tool that identifies network devices and their attributes, and provides recommendations for the DISA STIG policies that apply to each node based upon device type and software installed. Used in conjunction with SecureVue Auditor License, the STIG Profiler drastically reduces the amount of time required to identify which STIGs apply to which systems.



SecureVue STIG Profiler automates the profiling of devices on a network in preparation for a DISA STIG audit. Using the STIG Profiler, an IT Security Auditor can quickly identify all of the nodes on the network, scan the devices for detailed asset information, and generate a report of the applicable DISA STIG policies for each device.

Reports from the SecureVue STIG Profiler can be saved in .csv format and used to create a master node list for SecureVue to audit.



About EiQ Networks

EiQ Networks, a pioneer in security hybrid SaaS and continuous security intelligence solutions and services, is transforming how organizations identify threats, mitigate risks, and enable compliance. EiQ offers SOCVue, a security hybrid SaaS offering, and provides 24x7 security operations to Small to Medium enterprises who need to protect themselves against cyber attacks but lack resources or on-staff expertise to implement an effective security program. SecureVue®, a continuous security intelligence platform, helps organizations proactively detect incidents, implement security best practices, and receive timely and actionable intelligence along with remediation guidance. Through a single console, SecureVue enables a unified view of an organization's entire IT infrastructure for continuous security monitoring, critical security control assessment, configuration auditing, and compliance automation.

For more information, visit: http://www.eiqnetworks.com.