IMPROVE AND AUTOMATE COMPLIANCE WITH RED HAT AND OPENSCAP

A solution for healthcare providers

BRIEF

Red Hat and OpenSCAP provide a security hardening solution for Linux environments to help your organization:

- Regularly check systems against HIPAA and other security policies

- Automatically generate detailed scan reports

- Immediately repair issues

- Develop a baseline for compliance

- Monitor continuously to prevent drift

- Dynamically adjust policies and configurations

- Create customizable dashboards

- Reduce costs and efforts

PROTECTING PATIENT DATA IN A COMPLEX ENVIRONMENT

In today's healthcare environment, providers must strike an increasingly difficult balance: providing exceptional, affordable, value-based care to patients, while also keeping costs low and maintaining compliance with constantly changing federal privacy and security regulations. To stay competitive, many hospital systems are taking advantage of the power and flexibility of open source tools to develop the digital services its patients demand.

A powerful open source security solution is available from Red Hat and the OpenSCAP community, offering a security hardening solution for your IT environments that provides fast, verifiable, repeatable security for Health Insurance Portability and Accountability Act (HIPAA) compliance. This solution can help you:

- Meet HIPAA requirements to protect electronic-protected health information (ePHI) by performing regular risk analysis to ensure that safeguards, such as anti-virus software and role-based authentication policies are robust and up to date.

- Use technology to monitor and remediate vulnerabilities to keep you compliant, which is a time-consuming and difficult pursuit.

- Reduce the risk of additional theft or fraud, costly downtime, and significant financial penalties in the case of a large-scale data breach.

To help customers meet HIPAA and other governmental standards, Red Hat worked with the National Institute of Standards and Technology (NIST) to develop the Security Content Automation Protocol (SCAP). The leader in open source software offerings, Red Hat, teamed with OpenSCAP, the leader in open source security protocols, to provide the tools to help prevent, detect, and mitigate security threats.

SECURE YOUR INFRASTRUCTURE WITH OPEN SOURCE TOOLS

Now, by combining OpenSCAP and Red Hat® automation, you can take control of your organization's exposure by conducting regular security checks to find vulnerabilities within your network and immediately remediate any issues you find. This solution provides:

- **Scheduled vulnerability scans and detailed reports comparing your systems against a number of standards—including the recently added HIPAA profile** provided by OpenSCAP 1.2, a NIST-certified configuration and vulnerability scanner, bundled with Red Hat Satellite for Red Hat Enterprise Linux® 6- and 7-based systems.

- **A centralized web console to administer OpenSCAP profiles and the ability to identify vulnerabilities and patch, provision, and manage your Linux-based systems** provided by Red Hat Satellite.

- **A dynamic inventory to automate the remediation process so immediate action can be taken to address potential client issues** provided by Red Hat Satellite and Red Hat Ansible® Tower.
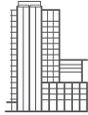
NORTH AMERICA
1 888 REDHAT1

EUROPE, MIDDLE EAST,
AND AFRICA
00800 7334 2835
europe@redhat.com

ASIA PACIFIC
+65 6490 4200
apac@redhat.com

LATIN AMERICA
+54 11 4329 7300
info-latam@redhat.com

facebook.com/redhatinc
@RedHat
linkedin.com/company/red-hat

- **Orchestrate across multiple front-end tools such as Windows, networking devices, and ServiceNow and an icon-based dashboard to run compliance checks at the touch of a button** with Red Hat CloudForms®, which is an optional, customizable self-service portal for either Satellite or Ansible Tower.

- **A vulnerability-free environment and immediate compliance at deployment** with Red Hat Enterprise Linux Anaconda installer.

BUILD IN AUTOMATED SIMPLICITY AND SECURITY

With Satellite, you can run vulnerability scans at any frequency. Scans return detailed reports that measure systems against a HIPAA profile and indicate which pass, which fail, and why.

OpenSCAP also automatically generates and passes customized playbooks to Ansible Tower, so you can immediately correct any issues identified in the scan. You can then make this automation part of a standard corporate build process. As a result, you can provision and deploy fully compliant, secure systems to your network from the start, using policies based on HIPAA.

OpenSCAP scans and reports also inform an audit process to help your organization track down and understand exactly where, when, and how vulnerabilities were introduced—including any new users or settings changes that may have appeared at the same time.

GUARD AGAINST CONFIGURATION DRIFT

Scheduling regular system checks provides you with up-to-date protection against new vulnerabilities and threats. It also returns your systems to your baseline, which prevents the drift that can occur as new software is added, existing software evolves, and as users log in and interact with the environment.

The combined solution can be dynamically configured to your existing systems and policy needs, and you can adjust policies to fit your organization's needs. With CloudForms, you can additionally create customized dashboards to make it easy for users to check specific systems as needed.

REDUCE COSTS AND EFFORT

Red Hat and OpenSCAP tools reduce the downtime and manual effort required during upgrades and updates, making the never-ending task of securing your environment easier, and in turn reducing costs.

OpenSCAP profiles and playbooks are available through Red Hat at no cost. Together, these tools offer you a security hardening solution for Red Hat Enterprise Linux that provides fast, verifiable, repeatable security for HIPAA compliance. Please contact your Account Representative to learn more.