



CASE STUDY

Automating security compliance activity

THE COMPANY

An insurance company serving more than 140,000 providers and over 7 million Insurance beneficiaries processes 130 million claims annually with more than \$47 billion in benefit payments.

Because the company has contracts with the Department of Defense, it must meet strict security regulations. It must comply with technical testing and hardening frameworks as STIG, or Security Technical Implementation Guide, which is published by the Defense Information Systems Agency, or DISA.

STIGs contain technical guidance to harden information systems/software that might otherwise be vulnerable to a malicious computer attack.” To date, DISA has released 461 STIGs, and continues to release more on a semi-regular basis.

THE NEED: Move away from manual processes

As part of their contract obligations, the insurance company is required to check and document prescribed Security Configuration Management information from their IT environment. This compliance activity includes providing evidence of DISA STIG checks on every host, application, network device and workstation they operate.

Tedious and time consuming, this process is critical to the company's federal contract business. Audit find-

ings and even financial penalties can be imposed if accuracy, timing, and quality reporting are not achieved.

Performing this work manually was a significant burden on the current IT staff, and the results

were inconsistent and often full of errors. The company needed a way to automate and build efficiencies into their audit process

to improve the overall accuracy of the results and deliverable report. Alignment with STIG values and CMS guidelines was critical to their evaluation as a provider and success with future contract awards.

THE SOLUTION:

Automated compliance documentation

LRS researched the STIG requirements, interviewed key application stakeholders at the company and reviewed its data collection processes over the course of many months.

The LRS team then designed an automated approach to accomplish these compliance checks with a fully managed service engagement. The services included understanding the specific STIG values, developing methodologies for success in assessing the environment, and creating custom automation to perform the required system checks in a more efficient manner. Being able to write the code

to automate the time-consuming tasks meant that LRS' team could reduce the amount of manual effort required and also ensure the accuracy and output values for the checks were drastically improved.

LRS worked alongside the company's application and compliance teams to develop a strategy for accomplishing goals.

Not only did LRS create a more efficient process for performing the work, we established a central reporting database for managing the compliance data and reporting automation. Additional features for quality control and device count accuracy were built into the design.

THE RESULT: Automation reduces documentation time

With LRS working alongside the company's application and compliance teams, we were able to develop a strategy for accomplishing the goals. As more automation was used, the level of effort by the insurer's application teams was reduced. LRS worked on new development of overall quality control, the check count and reporting variables become more consistent and accurate. This provided the client with a much higher level of confidence in their compliance reporting.



Learn more, visit LRSolutions.com or call 217.793.3800

©2022 All rights reserved. LRS is a registered trademark of Levi, Ray & Shoup, Inc. IBM, the IBM Premier Business Partner, POWER6, POWER7, and System i are registered trademarks and POWER 7 Systems is a trademark of International Business Machines Corporation in the United States, other countries, or both. NAL and North American Lighting are registered trademarks of North American Lighting, Inc.