KALLES GROUP
IT Professional Services

# Building and Deploying a Comprehensive PCI Auditing Program

Fashion retailer

## Challenge

As part of a massive effort around PCI compliance, a large retail company must meet and potentially exceed all PCI (payment card industry) requirements. In the past, parts of the company's infrastructure would be managed by centralized teams. Because the company is currently moving to an agile type of environment, every team must now take full responsibility for their infrastructure. The engagement involved a particular team that was still ramping up on the skillsets involved with this type of infrastructure management.

Furthermore, part of PCI compliance requires full logging for PCI systems and software. For this and other PCI requirements to be met, this team needed a full audit of current systems, automation for software deployment, and detailed configuration for disparate system-types to be migrated to a new logging infrastructure.

The team oversaw Identity and Access Management (IAM) across the company so the infrastructure was almost entirely PCI systems that were used for access. System monitoring and management was not in place for this team due to the current migration to agile methodologies.

## Approach

To migrate all systems to a new logging platform, each system must first be audited within the production infrastructure. While the PCI remediation team had already completed part of this, they were working with an older network scan that did not audit all the software on each device. In addition, each software type included different logging requirements and the logging system was paid by the terabyte, so each system had to be carefully measured for log value and size. Without a systems management infrastructure in place, this was the largest part of the project.

Once audited, Kalles Group focused on automating logging software installation and configuration. This not only significantly reduced the project timeline but also provided a manageable way for the team to install and configure the tool in the future. The company used Chef for most of its automation and the team would require detailed instructions on how to use it.

Once automation was complete and all systems had logging, a full audit of all PCI systems was required for proof. This process not only provided PCI evidence, but also surfaced problems such as firewall rules, automation bugs, and more. The entire project was completed in six weeks.

**Kalles Group**
www.kallesgroup.com

601 Union Street, Suite 4200
Seattle, Washington 98101

solutions@kallesgroup.com
206.652.3378

## Solution

Using PowerShell and an internal web API, all systems were audited for running processes. This revealed that less than 10% of the systems were logging as well as what processes were running that needed to be monitored and recorded. Using Chef for all Linux systems and PowerShell with a custom executable that installed and configured the Splunk client, all systems were able to have the software installed and configured.

Working with the team and compliance, Kalles Group was able to designate applicable and valuable logs. In addition, setting up dashboards in Splunk showed full PCI compliance evidence.

## Results

This same project was previously attempted but after six months, still had not been fully completed. Kalles Group was able to have all PCI systems logging and PCI-compliant within four weeks. All systems were audited and evidence was provided within another two weeks. The entire project was completed with a manageable automated solution and caused zero downtime to any systems.


Kalles Group was able to have all PCI systems logging and PCI-compliant within four weeks. The entire project was completed with a manageable automated solution and caused zero downtime to any systems.

**Kalles Group**
www.kallesgroup.com

601 Union Street, Suite 4200
Seattle, Washington 98101

solutions@kallesgroup.com
206.652.3378