CASE STUDY

LogRhythm Ensures Perfect Health for PCI DSS Compliance at St John Ambulance

Organisation
St John Ambulance
www.sja.org.uk

Industry
Charity

Employees
1,500

Solution Deployed
LogRhythm

Log Sources Include
- Routers
- Switches
- Firewalls

Key Impacts
- PCI compliance
- Network visibility
- Simplified Reporting
- Alerting on unusual behaviour on IT network

> “We evaluated a number of offerings but LogRhythm stood out as being more flexible and configurable than the others.”
>
> “Not only has LogRhythm ticked the PCI DSS compliance box for St John Ambulance, but it’s effectively keeping an additional watchful eye on network activity. ”
>
> *Karl Heydenrych*
> IT Director
> St John Ambulance

St John Ambulance is the nation’s leading first aid charity. The organisation helps people learn first aid so that they can be the difference between a life lost and a life saved. St John Ambulance teaches more people first aid than any other organisation, with over 800,000 people receiving training each year in schools, workplaces or in the community.

The challenge

St John Ambulance generates income through its first aid training programmes and supplies; service delivery programmes which provide first aid at public events; and through charitable donations. With around 80,000 card transactions per annum for these products, services and donations, the organisation is classed as a level three PCI DSS merchant and therefore must meet the necessary compliance mandates associated with the regulations.

These include specific requirements relating to how log data is handled such as the requirement that logs must be stored in a central repository and in an accessible format (requirement 10.) This also applies to files which are unlikely to be altered but still have to be monitored to guard against tampering.

Before LogRhythm, all log data at St John Ambulance was handled manually. In light of the PCI DSS requirements, it recognised that continuing with this approach would have an adverse impact on the organisation – either requiring additional costly resources or needing to divert existing IT infrastructure personnel from their current roles, putting a strain on network management and IT support activities.

The solution

Keen to automate the log management process, St John Ambulance assessed a number of products before selecting a security information event management (SIEM) solution from LogRhythm. The choice was based on the recommendation of Softcat, a provider of software licensing, hardware, security and related IT services as Karl Heydenrych, IT director, St John Ambulance explains:

“We have had a long and successful partnership with Softcat which means that the company has an excellent understanding of our operation and was therefore well-placed to advise on the different technologies available which could help meet our needs. As such, we fully trusted Softcat’s suggestion that we add LogRhythm to our shortlist of log data management solution providers.

“We evaluated a number of offerings, but LogRhythm stood out as being more flexible and configurable than the others which we felt would ensure a better fit for our business and bring a faster return on investment, which is important for us as a charity. Additionally, LogRhythm was the only solution we found which offered integrated File Integrity Monitoring. Not only would this negate the need for us to purchase an additional solution to meet the specific File Integrity Monitoring requirements (11.5) of PCI DSS, but it would simplify and strengthen our security, audit and compliance processes."

Implementation of LogRhythm was carried out by specialist security distributor and LogRhythm partner, Vigil Software. Following this initial installation, the system was regularly reviewed by Softcat and fine-tuned to ensure optimal performance. "Installation of LogRhythm was straightforward with no technical issues," continues Heydenrych. "Softcat has played an invaluable role in helping to scope out our requirements, proofing the concept and supporting us to get up and running with the new system."

The log data which relates to the PCI DSS regulations is generated by upwards of 400 heterogeneous devices, systems and applications at St John Ambulance, including routers, switches and firewalls.

LogRhythm automatically gathers the log data from each of these sources, archiving it to a central repository where it can be easily retrieved and reported on when required. Additionally, LogRhythm alerts on any unusual behaviour on any of these devices in line with PCI DSS requirements.

As a direct result of implementing LogRhythm, St John Ambulance is now fully PCI DSS compliant.

Heydenrych continues,

"As part of our corporate governance responsibilities, St John Ambulance places great importance on looking after its customers, donors and partners - including protecting the credit card details we process for each one. Not only has LogRhythm ticked the PCI DSS compliance box for St John Ambulance, it's effectively keeping an additional watchful eye on network activity. We get regular alerts on any abnormal activity, such as any attempts at external web-based attacks or to modify privileged accounts. These alerts reassure us that the protective measures we have in place are operating exactly as they should. Additionally, LogRhythm makes it quick and easy to produce detailed and easily-understandable reports as per PCI DSS requirements."

> " LogRhythm was the only solution we found which offered integrated File Integrity Monitoring. "
>
> *Karl Heydenrych*
> IT Director
> St John Ambulance

Now that the original objective of installing LogRhythm at St John Ambulance – namely PCI DSS compliance – has been met, the organisation is considering how it can develop the system further. Heydenrych concludes:

"LogRhythm can offer us much more than just PCI DSS compliance, for example, greater visibility of our IT infrastructure through a single dashboard. As such, we're working with Softcat to assess how best we can realise LogRhythm's full potential and look forward to rolling it out further across the organisation in the future."