CASE STUDY

Cardiff County Council - LogRhythm Combines GCSX and CoCo Compliance with Improved Reporting and Enhanced Network Permomance Analysis

LogRhythm

CARDIFF
CAERDYDD

Customer

Cardiff Council, County Hall
Atlantic Wharf
Cardiff CF10 4UW
www.cardiff.gov.uk
The county of Cardiff is the largest in Wales in terms of population, delivering services to approximately 320,000 people.

Industry

Public Sector

Employees

Approximately 18,000

Log Sources Include

- Active directories
- Exchange Server
- Nortel Virtual Private Network
- Citrix Active Gateway
- Safeword two factor authentication
- Check Point firewall

Key Impacts

- Reduction by hours of daily log data audits
- Simplified log data analysis
- Improved visibility of data centre activity
- New network management efficiencies
- Optimum levels of security resulting in improved customer service

> "LogRhythm is easy and intuitive to use and has been imperative to Cardiff County Council achieving CoCo and GCSX compliance."
>
> *Mike Selley*
> IT Service Delivery Manager
> Cardiff County Council

The introduction of the Government Connect Secure Extranet (GCSX) and Code of Connection (CoCo) initiatives in the U.K. signalled the need for Cardiff County Council to re-evaluate how it handled its log data. Since installing a log data management, analysis and event management solution from LogRhythm, Cardiff County Council has not only achieved GCSX and CoCo compliance, but has improved its reporting mechanisms and enhanced network performance analysis.

Like all English and Welsh local authorities, Cardiff County Council was urged to join the UK GCSX initiative aimed at creating a private wide area network for secure communications between connected government organisations. As part of this, local authorities must sign up to the Code of Connection (CoCo) which includes specific requirements on log data.

Cardiff County Council already had its own manual, decentralised log data solution but this was complex and time-intensive to use. The Council recognised that a more sophisticated solution could streamline this process extensively.

Comprehensive and flexible search capabilities

Cardiff County Council evaluated offerings from three players in the market before selecting LogRhythm. Andrew Horner-Seddon, principal IT consultant – Security, Cardiff County Council explains:

"Some of the solutions we looked at provided log data indexing but the data could only be searched on by using specific index codes. LogRhythm offers a much more comprehensive and flexible search capability which makes it significantly quicker and easier to find information and run reports. We also like the fact that LogRhythm provides an integrated hardware and software solution which gives a clear understanding of the total investment needed over time."

LogRhythm's log and event management solutions hone in on security threats and operational risks in a fraction of the time compared to conventional log search utilities. LogRhythm goes beyond simple indexing, enriching log entries with intuitive classifications, human understandable names, risk modelling and prioritization and a universal time stamp.

Centralised Storage

At Cardiff County Council, LogRhythm monitors, extracts and centrally stores log data from the council's active directories, Microsoft Exchange server, Virtual Private Network (VPN), Citrix Active Gateway, Safeword two factor authentication solution and Check Point firewall.

Powerful reporting couple with real-time alerts

LogRhythm's primary use at Cardiff County Council is for reporting purposes. These reports – which, instead of taking days, can be produced within a matter of minutes or hours depending on their complexity - are used to report from both operational and technical perspectives.

> "LogRhythm offers a much more comprehensive and flexible search capability which would make it significantly quicker and easier to find information and run reports."
>
> *Andrew Horner-Seddon*
> Principal IT Consultant, Security
> Cardiff County Council

Andrew Horner-Seddon continues:
"LogRhythm has been invaluable in helping us identify issues across our domain controllers. We use it to automatically generate reports every week to give us an unprecedented insight into domain activity, for example, we are able to tell if accounts have been created or deleted or if users are violating their network privileges. We can even see if any areas of the network are under pressure so that we can take the necessary action to avoid a potential problem in the future. LogRhythm's reports are straightforward, easy to read PDFs and the information they hold is extremely powerful. We can also automate them to save on our file server where they can be accessed by others if permitted and act as an additional layer of backup if required."

As well as using LogRhythm for generating reports on historical activity, the IT department also relies on it to provide real-time alerts on unusual activity on the network. For example, if there has been irregular overuse of the system such as increased instances of attempted log-ins over a period of time which may signify a virus attack or attempted security breach.

Mike Selley, IT service delivery manager, Cardiff County Council concludes:
"LogRhythm is easy and intuitive to use and has been imperative to Cardiff County Council achieving CoCo and GCSX compliance. The real-time alerting feature is useful and interesting in equal measure, while the various reporting mechanisms including dashboard monitoring give us easier access to a deeper and wider source of data. Legally, we have to keep six month's worth of log data on the system. Now that we've almost hit this level, we're starting to look at how we can extend LogRhythm to other aspects of our operation, for example helping the Council comply with the Payment Card Industry Data Security Standards (PCI DSS) or extending LogRhythm's reach into the internet log data generated."

> "The real-time alerting feature is useful and interesting… while the various reporting mechanisms including dashboard monitoring give us easier access to a deeper and wider source of data."
>
> *Mike Selley*
> IT Service Delivery Manager
> Cardiff County Council

©2012 LogRhythm Inc. | LogRhythm_Cardiff_Case_Study_12.12