**Case study**

**Bank AlJazira**

*HP Enterprise Security Customer Case Study*

**Industry**  
Banking and Financial Services

**Objective**  
Centralize security event administration for corporate datacenter and branch offices in order to gain comprehensive event analysis and accelerate the time to resolve security issues

**Approach**  
Work with HP partner, IT Security Training & Solutions, to implement HP ArcSight universal log management solution

**IT matters**

- Bank AlJazira has greatly reduced its security event administration efforts due to HP ArcSight PCI Logger centralized log management and analysis capabilities.
- HP ArcSight PCI Logger has enabled Bank AlJazira to unify searching, reporting, alerting and event analysis for all enterprise log data for the corporate datacenter, as well as its growing number of branch offices.

**Business matters**

- HP ArcSight PCI Logger was a key factor in Bank AlJazira’s ability to achieve PCI certification, which occurred within three months of deploying the solution.
- Consolidation of all logs in a consistent format enables Bank AlJazira to conduct faster, comprehensive event analysis and accelerates the time to resolve security issues.

“HP ArcSight PCI Logger has enabled our security team to quickly respond to any threats and be proactive about possible issues and incidents. This significantly lowers our risk of data loss, preserving our excellent reputation for ensuring client data security in the financial services market.”

– Mr. Muhannad Zghoul, IT Project Manager, Bank AlJazira

As one of Saudi Arabia’s leading financial institutions, Bank AlJazira is continually looking for new ways to improve and streamline its IT operations and protect confidential client data. But with a rapid growth rate and the recent introduction of several new service offerings, the bank’s IT security team was facing several serious challenges.
The Bank AlJazira challenge

Bank AlJazira’s growing base of 55 branch locations and critical systems that store, process and/or transmit cardholder information rely on the bank’s centralized IT resources. Bank AlJazira maintains a complex heterogeneous environment of servers and security devices, so its major technical challenge was the lack of a unified logging policy and incompatible log formats across devices. Many of the branch office systems required the involvement of local device owners to obtain access to logs, and it would often take a significant amount of time to identify, analyze and respond to a single issue, particularly when there were many different systems and applications involved.

Bank AlJazira also required a log management solution due to the Saudi Arabian Monetary Agency (SAMA) mandate to comply with Payment Card Industry (PCI) requirements. A centralized logging system would enable Bank AlJazira to obtain the necessary certification. We needed a consistent and centralized logging framework to achieve PCI regulatory compliance and speed our response to any security events,” explains Mr. Muhannad Zghoul, IT Project Manager and core team member of the PCI program at Bank AlJazira.

The HP ArcSight impact

HP ArcSight PCI Logger has enabled Bank AlJazira to unify searching, reporting, alerting and event analysis for all enterprise log data for the corporate datacenter, as well as its growing number of branch offices.

“With the centralized logging and analysis enabled by HP ArcSight PCI Logger, the administrative burden on our security team has been greatly reduced,” says Zghoul. Bank AlJazira has also eliminated the need to rely on individual IT system owners to track and investigate events. Security administrators and IT team members are now able to shift their focus to more strategic activities, rather than spending their days monitoring thousands of separate logs for cyberthreats.

Faster and more accurate log analysis has improved data security for the bank. “HP ArcSight PCI Logger sends automatic alerts when any suspicious system activities occur, enabling us to easily pin-point the source of a problem and prevent security breaches,” says Zghoul. “Event identification and resolution processes that previously took a significant amount of time have been reduced considerably.”

The advanced functionality of HP ArcSight PCI Logger has been a key factor in the bank’s ability to achieve PCI certification and compliance. Interactive and personalized dashboards combine relevant PCI reports into a single role-based view. Reports can be analyzed using an intuitive search interface to conduct ad hoc investigations for root cause analysis and instant notification. Security administrators can quickly drill down from the report to identify the underlying events that triggered the alert.

With HP ArcSight PCI Logger, the bank has also been able to reduce its hardware infrastructure and support costs. All aggregated logs are stored on HP ArcSight PCI Logger in a compressed format (10:1 ratio), and log retention policies are automatically enforced. “With HP ArcSight PCI Logger, we no longer need to store logs related to PCI on each individual system,” says Zghoul.

“HP ArcSight PCI Logger has increased the ability of our security team to quickly respond to any threats and be proactive about possible issues and incidents. This significantly lowers our risk of data loss, preserving our excellent reputation for ensuring client data security in the financial services market,” Zghoul concludes.

The HP ArcSight solution

Bank AlJazira began its search for a centralized log management solution by identifying key selection criteria. The solution needed to be a best-in-class market leader with the ability to comply with PCI and other banking regulations. And, the vendor needed to demonstrate a very strong local presence and extensive, proven experience in the industry.

HP ArcSight emerged as the clear winner. “HP ArcSight PCI Logger is a well-known product, with a long history of successful implementations in the financial services sector,” says Zghoul.

Bank AlJazira chose to work with IT Security Training & Solutions (I(TS))², an HP ArcSight partner, to speed implementation and leverage industry best practices. I(TS)² is the Middle East’s premier provider of integrated security solutions, security consulting services, security training and certification curriculum, and managed security services. “I(TS)² has brought an unmistakable value to our HP ArcSight implementation,” explains Zghoul. “Their local support and knowledge has contributed greatly to our success.”
About Bank AlJazira:

Bank AlJazira is one of the fastest growing Shari'ah compliant financial institutions in Saudi Arabia. The bank’s activities are organized into five main sectors: retail banking, corporate banking, brokerage, treasury and Takaful, an insurance concept which conforms to Islamic rules and regulations. Bank AlJazira currently serves its client base through a network of more than 55 branches spread throughout the Kingdom of Saudi Arabia.

Customer at a glance:

Product

• HP ArcSight PCI Logger