opentext™ | Cybersecurity

Case Study

Kuwait Finance House

ArcSight supports advanced breach defense and full regulation compliance in evolving threat landscape with powerful real-time data correlation.

Overview

Kuwait Finance House (KFH) is considered a pioneer in the banking phenomenon known as Islamic Finance or Shari'a Compliant Banking. KFH is the first Islamic bank established in 1977 in the State of Kuwait and today it's one of the foremost Islamic financial institutions in the world. KFH has steadily expanded its business and achievements to lead the Islamic banking industry and become a pioneer financial establishment. KFH's group banking network spans across several regions worldwide, with 504 branches, 1,263 ATMs, and approximately 15,000 employees

Challenge

KFH, as all other leading financial institutions, was facing a growing cyber threat landscape and Mr Majeed Behzadi, Executive Manager, Group Information Security Management and IT Infrastructure Design for KFH, explains why the organization felt compelled to look for a comprehensive security solution: "We had a basic security monitoring solution but it didn't give us the correlation capabilities we felt we needed in a much more sophisticated threat landscape. There was also limited development and support on the solution, and we wanted to look for an alternative before ending up with an obsolete solution. We need to comply with very strict financial services industry regulations, including PCI-DSS, and we have a requirement to manage a Security Information and Event Management (SIEM) environment with 24/7 monitoring. We are also audited regularly and need to provide comprehensive reporting in support of this."

"Through the ArcSight Marketplace and Activate framework, we benefit from security rule-sets, dashboards, and reports developed by Micro Focus (now part of OpenText) SOC experts and the ArcSight Community. It has hugely enriched and enhanced our security operations and response times."

Mr Majeed Behzadi
Executive Manager, Group Information Security Management and IT Infrastructure Design
Kuwait Finance House

Solution

After a thorough market evaluation, the team concluded that ArcSight Enterprise Security Manager (ESM) in combination with ArcSight Logger was the best fit for their breach defence and compliance needs. ArcSight ESM provides powerful insight into real-time correlation of security events, while ArcSight Logger delivers a cost-effective universal log management solution that unifies searching, reporting, alerting, and analysis across any type of enterprise machine data. It has built-in content for regulatory and security compliance requirements to ease the burden on KFH's security teams.

بيت التمويل الكويتي
Kuwait Finance House

At a Glance

Industry

Financial Services

Location

Kuwait

Challenge

Gain enterprise-wide infrastructure visibility to enable fast and effective response to any cyber security threats

Products and Services

ArcSight Enterprise Security Manager (ESM)
ArcSight Data Platform (ADP)
ArcSight Logger
ArcSight Activate Content Packages

Critical Success Factors

- Full infrastructure coverage and visibility in SIEM environment
- Full compliance with industry regulations
- Comprehensive security reporting
- Fast and effective response to any threats

“The ESM correlation engine is one of the best in the industry. For our threat investigations it’s really helpful to collect data and correlate events in real-time to prioritize and escalate threats that violate the internal platform rules.”

Mr Majeed Behzadi
Executive Manager, Group Information Security Management and IT Infrastructure Design
Kuwait Finance House

Connect with Us
www.opentext.com

KFH engaged with a local implementation partner and within two months the ArcSight-driven SIEM environment was live. Set up in a datacenter-based cluster environment, disaster recovery is guaranteed through a separate site set up.

Mr Behzadi on how ArcSight supports the day-to-day operations within the KFH Security Operation Centre (SOC): “The ESM correlation engine is one of the best in the industry. For our threat investigations it’s really helpful to collect data and correlate events in real-time to prioritize and escalate threats that violate the internal platform rules. We were able to optimize the events received from the different sources using ADP filtering and aggregation capabilities, resulting in us only managing around 3,000 events per second. Thus, directing our resources in the right way is a key benefit for us.”

Mr Behzadi also found the community-driven ArcSight content to be of help: “Through the ArcSight Marketplace and Activate framework, we benefit from security rule-sets, dashboards, and reports developed by Micro Focus (now part of OpenText) SOC experts and the ArcSight Community. ArcSight Activate includes hundreds of use case solutions and ESM packages that we can simply download and integrate into our own ESM environment. It has hugely enriched and enhanced our security operations and response times.”

The reporting modules within ArcSight ESM and Logger have also been very useful.

The KFH security team have been able to introduce comprehensive dashboard reporting which is used in many parts of the organization, as well as in audits. Standard and custom, as well as automated and ad-hoc reporting are all part of the security service.

KFH have leveraged ArcSight to integrate with many financial applications. This makes adding digital payment capabilities seamless and simple by removing data silos and using customer data for real-time payments. It has helped minimize online fraud and ensures data confidentiality.

KFH have created an integrated enterprise software platform that brings together proven, real-time core processing with channel solutions from Finastra, a unique cloud platform built specifically for the financial market. This ensures that consistent information is available throughout the entire enterprise and that adding and maintaining customer records is simplified and streamlined. It improves compliance, as reporting and analysis is also made easier with drag and drop report-building capabilities from within the same database.

ArcSight Flex connectors for these use cases were developed through OpenText™ Professional Services and are available through ArcSight Marketplace. KFH leverages these concepts in advanced use cases to correlate the IT/security logs with financial data to cross verify attacks and identify vulnerabilities.

Results

KFH’s main objectives were to be fully compliant and have complete visibility of their infrastructure, improving their ability to respond in a timely manner to any threat events. Mr Behzadi is confident this has been achieved: “It’s hard to measure success in this area for us, but our entire infrastructure with all its elements is now 100% covered by our ArcSight-driven SIEM. Any future devices or systems can easily be integrated as the Internet of Things (IoT) becomes more relevant in our industry. We are fully compliant with any industry regulations and feel confident we can respond quickly and accurately to any security threats.”

The KFH security team is also looking into adding ArcSight Data Platform (ADP) to its SIEM. This will enable KFH to easily collect, normalize, enrich and distribute their event data to any other data consumers they may have, including their analytics tools.

Mr Behzadi concludes: “We want to expand our SIEM to provide a group level security service, centralized in Kuwait, to encompass our banking and non-banking subsidiaries. With our ArcSight implementation we feel ready to tackle this new challenge in an evolving threat landscape. ArcSight has helped us meet all compliance mandates in order to mitigate the risk of fines and potentially negative legal ramifications. We look forward to our continued partnership with Micro Focus (now part of OpenText).”

opentext™ | Cybersecurity

OpenText Cybersecurity provides comprehensive security solutions for companies and partners of all sizes. From prevention, detection and response to recovery, investigation and compliance, our unified end-to-end platform helps customers build cyber resilience via a holistic security portfolio. Powered by actionable insights from our real-time and contextual threat intelligence, OpenText Cybersecurity customers benefit from high efficacy products, a compliant experience and simplified security to help manage business risk.