

King Fahd University of Petroleum and Minerals

HP Enterprise Security Customer Case Study

“ArcSight ESM shows us prioritized articulation of security events; the way it automates is very impressive. We can now pinpoint any events that diverge from our security policy and remedy them with very little effort.”

—Mir Ahmed Ali Shajee, Technical Manager of IT Security,
King Fahd University of Petroleum and Minerals



Customer Brief

King Fahd University of Petroleum and Minerals (KFUPM) is one of the leading research and teaching institutions in the Middle East. Located in Dhahran, KFUPM plays an important part in the successful management of Saudi Arabia's vast petroleum and mineral resources - a complex and exciting challenge for scientific, technical and management education in the Kingdom of Saudi Arabia. To meet this challenge, the university offers advanced training in the fields of science, engineering and management in order to promote leadership and service in the petroleum and mineral industries. The university also furthers knowledge through research in these fields. In 2009, KFUPM was ranked 266 out of 30,000 selected universities worldwide by Times Higher Education-QS World University Rankings, based on research quality, teaching quality, employability of alumni and international outlook.

Product(s)

- ArcSight ESM

Business Benefits

- Through real-time, full-extent visibility of network activity, ArcSight ESM enables KFUPM to protect the integrity and availability of their critical assets
- The ArcSight ESM correlation engine makes it possible for KFUPM to pinpoint any events that diverge from its security policy in real time and remedy them with very little effort
- KFUPM is able to maintain a proactive security governance, taking into account both the openness needed for education purposes and rigorous security best practices



The KFUPM Challenge

As a top ranked university in the Middle East, KFUPM must ensure the integrity of its network while also allowing appropriate access to information as per the standards of a higher learning institution. The university is managing a complex and heterogeneous IT environment with a dynamic, technologically advanced student population. KFUPM needed a fully featured information security monitoring platform for proactively identifying and remediating any security threats before they could be exploited by internal or external sources.

KFUPM realized that being able to see clearly what was happening across all network systems and devices in real time was paramount to effectively prevent sophisticated cybersecurity breaches. In particular, it was concerned about the effects of malware on its network. The Conficker worm, which in 2009 spread rapidly into one of the largest worm infections in history, attacked more than seven million computers in over 200 countries. The worm was unusually difficult to counter because of its combined use of many advanced malware techniques.

HP Enterprise Security Customer Case Study

Study: With ArcSight ESM, KFUPM can clearly see what is happening across all network systems and devices, and is effectively preventing sophisticated cybersecurity breaches from occurring.

Industry: Education



“Right around the time we identified the need for more accurate and complete visibility into our network, the Conficker worm began spreading worldwide,” says Mir Ahmed Ali Shajee, Technical Manager of Security for KFUPM. “We absolutely needed to guard against that type of cyberthreat and any others that could manifest.”

The ArcSight Solution

KFUPM investigated options for intelligently correlating network events and gaining the visibility it needed to protect the university’s critical systems and reputation. Based on extensive analysis and an internally developed proof of concept, KFUPM selected ArcSight ESM. Though other products on the market such as RSA enVision made it onto the short list, ArcSight ESM proved to be superior as reported by trusted security industry analysts and consultants.

“We didn’t go through an extensive effort to settle on the second-best option,” says Mir. “ArcSight ESM is simply the best SIEM solution on the market and provides all the automation and features we could hope for.”

I(TS)² (IT Security Training & Solutions), an ArcSight partner, was involved early on in the selection process. 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. Its unrivaled regional knowledge along with the market-leading ArcSight SIEM solution was a winning combination.

ArcSight ESM provides a single management platform that monitors all events across the organization and uses powerful correlation and analysis to identify cyberthreats. KFUPM integrated ArcSight ESM with their existing intrusion prevention system, vulnerability scanner, firewalls, proxy servers, Active Directory domain controllers and end point security suites.

The ArcSight ESM real-time event management provides accurate, automated prioritization and useful data that can be leveraged in security risk mitigation. As a result, KFUPM can respond immediately to suspicious activity and take corrective action before it manifests into a more serious situation.

The ArcSight Impact

As part of the ArcSight ESM deployment process, I(TS)² helped KFUPM identify their key assets so that risk prioritization could aid in identifying only the real threats that needed attention. Prior ArcSight ESM, security staff at KFUPM reviewed logs manually, a time-consuming task that did not honor their advanced skill sets. Even so,

the security department had to make some judgment calls, as the volume of events was staggeringly high. For example, Mir and his team configured the firewalls very tightly and would regularly audit them, but forego the task of reviewing the logs in real time. It also was not easy to pinpoint issues by reviewing syslogs. However with ArcSight ESM, KFUPM security specialists can quickly put their fingers on any potential cyberthreats or anomalies that need attention.

“ArcSight ESM shows us prioritized articulation of security events; the way it automates is very impressive,” says Mir. “We can now pinpoint any events that diverge from our security policy and remedy them with very little effort.”

In particular, Mir likes the ability to create event graphs on an ad hoc basis for viewing and identifying patterns of suspicious activity. It was through an event graph that Mir was alerted to the magnitude and spread of the Conficker worm and its evasive activities. He was then able to isolate the problem and remediate it before the university’s critical assets were compromised.

ArcSight ESM real-time security monitoring also provides KFUPM with the ability to protect the confidentiality, integrity and availability of their networks, systems and applications. Logs from the university’s Cisco firewalls had been generating events that were policy violations; they were of course denied and presented no real threat. But what KFUPM didn’t focus on earlier was how those attempts impacted the computer network.

“From our proof of concept we were able to identify certain machines, dumb terminals, that had become infected and were spreading malware across the network,” says Mir. “With ArcSight ESM, we were able to capture the problems and remediate the systems, which improved the performance and reliability of our network.”

ArcSight ESM has enabled KFUPM to comply with its own rigorous security policy while also enabling maximum flexibility and openness for student learning, research and collaboration. Support from Sadiq Sait, Professor and CIO at KFUPM, and diligent efforts of the security team, especially Aiman Rasheed and Khawar Khan, were key to the project’s success.

“Our experience with ArcSight is outstanding,” says Mir. “The local support from I(TS)², along with education courses and Internet-based support from ArcSight, have enabled us to adopt best practices and maintain a proactive security posture.”

