

Case Study: Iberdrola

“ArcSight ESM made an immediate impact on our business, delivering the highest level of protection against internal and external threats right across our global network. Moreover, by automatically identifying, correlating and prioritizing security events, ArcSight has increased the efficiency of our IT department by eliminating false positives and reducing the number of critical alarms.”

Francisco J. García-Carmona, Head of IT Security, Iberdrola

Impact Highlights

- Enables Iberdrola to react promptly and effectively to attacks and abnormal situations across the global organization
- Provides Iberdrola with a significant improvement in its ability to filter and correlate the 15 million security events
- Provides Iberdrola with a clear view of its threat exposure to reduce corporate and IT risk

About Iberdrola

With a 100 year heritage, Iberdrola is one of the world’s largest private energy utilities—reaching over 16 million customers. Iberdrola is committed to the promotion and adoption of the best practice in Corporate Governance across its international businesses. The consolidation and management of its security portfolio through the implementation of the ArcSight ESM was the next step in the company’s strategic governance program.

Iberdrola’s Challenge

With multiple business units, servicing millions of customers across the world, Iberdrola faced a common challenge; namely, the sheer volume of security information generated by the myriad of devices across its network. Indeed, Iberdrola estimates it receives over 15 million security events on its network each day. To achieve its Corporate Governance targets and guarantee the highest level of organizational security, Iberdrola needed to address this issue and consolidate its security related information into an easily understood and manageable format.

Iberdrola demanded complete clarity of its security environment to assess and reduce its threat exposure by reacting promptly to attacks or abnormal situations and to control and measure the efficiency of its security devices and policies. In support of its Governance commitment, Iberdrola also required this comprehensive view to build management and performance measurement systems.

Iberdrola’s experienced team initially investigated nine technologies that represented the best solutions available in the market. After a comprehensive five month selection process based on criteria including; functionality, stability, scalability, ease of integration, technical ability of service provider, vendor product roadmap and total cost of ownership (TCO), ArcSight and one other vendor were approached to deliver a trial deployment. After an incredibly successful trial, ArcSight came out on top.

“ArcSight was chosen as the preferred supplier for two simple reasons,” says Francisco J. García-Carmona, Head of IT Security at Iberdrola. “First, it was clear that ArcSight has developed the market’s most comprehensive security information management solution for large, global enterprises. Secondly, its integration partner Breyer was particularly convincing in its ability to demonstrate technical expertise and the required degree of specialization.”



The ArcSight Solution

The ArcSight solution met Iberdrola's specific selection criteria. The project captured and consolidated all security information across the Iberdrola global network, and provided real-time analysis of the log information obtained from all of its communications and IT security devices, operating systems and applications. The defining feature that led Iberdrola to the ArcSight solution was its comprehensive capabilities in the face of complex needs that this utility business demanded.

Iberdrola bought the first of its 300 licenses in December 2004 after the successful completion of the trial deployment. "It was vital to get the basics right, and the most time consuming task was the high level analysis of the volume and structure of the information that needed to be consolidated. In addition, ArcSight ESM had to be integrated seamlessly with existing systems management applications and infrastructure used by Iberdrola," says Jose M. Bermudez, CEO of Breyer, ArcSight's certified partner in Spain. "The time invested in the analysis, and the flexibility and scalability of the product ensured a quick and hassle free deployment."

"The overall quality of the ArcSight solution and the high level of expertise of the engineers involved in the planning and implementation phases not only allowed us to achieve initial targets, but also led to an improvement in our ongoing deployment strategy. This experience, and ArcSight's knowledge of the platforms and environments involved, significantly shortened implementation time," comments García-Carmona.

The ArcSight Impact

ArcSight ESM made an immediate impact on Iberdrola's business. The utility has seen huge improvements in its ability to filter and correlate the massive volume of data that once threatened to drown the security function. Critical alarms are now relatively rare as ArcSight automatically identifies and prioritizes security events, and eliminates the hours associated in chasing down hundreds of false positives. In fact, Iberdrola began to detect very significant improvements in the efficiency of its IT Security department immediately after the initial deployment.

The sheer power of the ArcSight solution and the knowledge and experience of Breyer in the development of large and technically complex projects added value throughout the project. Iberdrola was particularly impressed by the speed of the deployment and the ease of integration into its existing IT environment.

In addition, ArcSight has now brought a previously unachievable level of clarity to Iberdrola's security environment. Its consolidation and correlation functionality is delivering a comprehensive understanding of internal and external threat activity, to accurately gauge threat exposure and enable the correct remedial action to be taken.

"Building up a clear picture of our vulnerabilities across the global network has allowed us to employ new processes and activities that significantly reduce the risk of attack," says García-Carmona. "This is fundamental in protecting our network from insider and outsider threat, but also enables us to report against such actions to ensure Iberdrola's Governance standards and policies remain some of the most rigorous in the industry. Tight control of the security environment is also vital as Spain has historically faced home-grown and external terrorist activity, and utilities are seen as strategic targets."

While Corporate Governance and increased efficiencies of the IT team are of paramount importance for Iberdrola, security chief, García-Carmona, is clear on the most fundamental benefit of ArcSight. "We know the TCO of our IT security infrastructure and the benefits to be obtained from an improvement in our capability to manage and exploit these assets. However, we are also very aware of the risk of exposure, and the financial and organizational cost of a security incident detected too late. With 16 million customers to service, we simply cannot afford not to protect the network, and for this reason put our trust in ArcSight." That trust, concludes Breyer's Jose Bermudez, has been well earned and repaid time and again.

About ArcSight

ArcSight provides real-time threat management and compliance reporting by collecting, analyzing and managing security data. ArcSight ESM™ enables global companies and government agencies to centrally and more efficiently manage information risk.

ArcSight, Inc.

5 Results Way, Cupertino, CA 95014, USA
www.arcsight.com / email: info@arcsight.com
Corporate Headquarters: 408 864 2600
EMEA Headquarters: +44 870 351 6510
Asia Pac Headquarters: 852 2166 8302

© 2005 ArcSight, Inc. All rights reserved. ArcSight and ArcSight ESM are trademarks of ArcSight, Inc. All other product and company names may be trademarks or registered trademarks of their respective owners. 10/05