KoçSistem

Protecting assets and information from advanced threats

Overview

The need
KoçSistem's previous SIEM system was difficult to deploy, use, maintain, and integrate with other applications, which increased training and staffing costs, and impeded compliance processes.

The solution
KoçSistem replaced a complex system with an advanced QRadar SIEM solution from IBM that helps staff cost-effectively address internal and external security threats and meet local Internet regulations.

The benefit
The IBM solution provided a lower total cost of ownership, increased performance and improved ease of use compared to the previous solution.

KoçSistem is a leading cloud services company in Turkey, providing information technology consulting, systems integration, and IT solutions. The company is part of Koç Holding A.Ş., and employs approximately 1,500 people.

Controlling increased costs and complexity

In 2014, KoçSistem submitted a request for proposal (RFP) to security vendors to replace its SIEM system. Security Operations Center (SOC) staff found its existing SIEM system difficult to deploy, use and maintain, which increased training and staffing costs significantly. Additionally, staff reported challenges in adding timestamps on the captured logs via a custom-developed application—a necessity to address Turkish Internet compliance regulations. "As a security services provider, our main cost is staffing," says Serkan Özden, unit manager, Security Services, KoçSistem. "The more complex the product, the more training and specialized knowledge we need, which increases our costs."

Simplifying security surveillance

KoçSistem selected IBM® Security QRadar® SIEM following a Proof of Concept (POC) demonstration with several vendors. The software collects and correlates logs from more than 500 server and network devices, and processes approximately 20,000 events per second (EPS) to help SOC staff detect and prioritize security threats in near-real time. The solution also integrates with the company's electronic timestamp application to support local regulatory requirements.

Working with IBM has helped KoçSistem expand its services. "We now have a big project with one of Turkey's big retailers to provide security monitoring," says Serkan Özden, unit manager, Security Services, KoçSistem. "We are providing first- and second-level monitoring, and IBM provides level-three analysis and monitoring through its security operations center."

"We are integrating QRadar with our perimeter solutions, our security devices and our network access control solution to help us better cope with internal and external security threats," says Özden.

Reducing costs while supporting compliance requirements

"We've gained lots of benefits since we deployed the QRadar environment," says Özden. "The EPS cost is a minimum and the performance is very good compared to other products. We've also been able to address local regulations using QRadar with our electronic timestamp technology."

Additionally, the system's ease of use has reduced staffing costs. "Ease of use is an important requirement for us and it's one of the benefits that IBM QRadar provides," says Özden "We don't need to provide staff with as much training, and management of the device is not as complex, which reduces our personnel costs."

Solution components

Software
• IBM® Security QRadar® SIEM
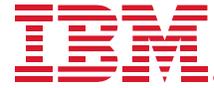
Services
• IBM Security Services

Take the next step

To learn more about IBM Security software, please contact your IBM representative or IBM Business Partner, or visit the following website:
ibm.com/security

For more information about KoçSistem, visit: www.kocsistem.com.tr

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

WGC12406-USEN-00