“Due to the intelligent aggregation and correlation capabilities of ArcSight ESM, our security events have been reduced from 550 million per week to just 50,000—achieving an incredible efficiency increase of 11,000 to one.”

– Manfred Troeder, Senior Manager of Global Security Operations Centre, Vodafone Group Services

Vodafone is a global telecommunications company headquartered in London. It operates in more than 30 countries and partners with other network providers in over 40 additional countries. As one of the world’s largest mobile communications companies, Vodafone provides mobile networking services to more than 359 million customers around the world. Vodafone has served as one of the industry’s earliest pioneers in mobile communications, starting with the world’s first mobile call in January of 1985. Today, Vodafone is more than just a cellular provider – customers in many markets also look to Vodafone for great value in their fixed line and broadband services as well.
Case study | Vodafone

The Vodafone Challenge

In order to support its large installed base, Vodafone relies on four very large datacenters with well over 20,000 servers and a heterogeneous collection of telecommunications infrastructure. To address security issues, Vodafone deployed state-of-the-art firewall, IDS/IPS, and anti-virus technology at each of its many locations around the globe.

The Vodafone Global Security Operations Centre (GSOC) serves as the centralized location where all of the separate data centers and offices feed in their security information for analysis. But due to the enormous magnitude and diversity of the company’s worldwide operations, all of the different IDS, firewalls, and antivirus systems were producing an overwhelming number of security events.

“Our company has grown very rapidly over the past few years,” says Manfred Troeder, Senior Manager of Network Security for Vodafone. “We have a ‘zoo’ of widely different security systems from a variety of vendors deployed in our environment.” Consequently, one of the company’s biggest challenges was to integrate these different products into a single GSOC. It was becoming almost impossible for the company’s security analysts to correlate, analyze and prioritize the plethora of security events in a timely manner, and to see an overall picture of the security situation across the enterprise.

As an industry leader, Vodafone is continually focused on improving its security operations. “Every single security event needs to be analyzed to identify potential security breaches or attacks,” says Troeder. “We need the ability to quickly identify redundant information and reduce false positives to a minimum, enabling our security analysts to focus on just the real, highest priority events.”

The ArcSight Solution

Vodafone evaluated several security information and event management (SIEM) products and found the ArcSight Enterprise Threat and Risk Management (ETRM) platform to be the absolute best solution for its needs. The ArcSight ETRM product suite provides complete visibility into all security activity across Vodafone’s IT infrastructure, including external threats such as malware and hackers, and internal threats such as data breaches.

Vodafone started with an implementation of ArcSight ESM, the industry-leading SIEM solution, in one of the company’s central datacenters. This implementation was then followed by a deployment of ArcSight Logger, the industry’s first universal log management solution that unifies searching, reporting, alerting, and analysis across all Vodafone enterprise log data.

The ArcSight Impact

With ArcSight ESM, Vodafone now has the ability to quickly identify suspicious behavior or cyberattacks, and can initiate the necessary responses immediately. “We can also easily report on our security situation on a regular basis,” says Troeder. “The ArcSight ETRM platform assures us the best deployment of our enterprise security budget.”

By using the ArcSight ETRM platform, Vodafone is able to link all of its different security products to the company’s centralized GSOC in a seamless manner. The company now has a real-time overview of its security situation across the enterprise. “All security events are aggregated and harmonized with ArcSight ESM,” says Troeder. “Our security analysts can easily analyze all of the events from each of the different security systems – even without specific knowledge of each and every product.”
Customer at a glance:

Solution
- ArcSight ESM
- ArcSight Logger

Perhaps the most tangible results Vodafone has experienced with the ArcSight solution are the efficiency improvements. For example, with the ArcSight ETRM platform the number of false positives and redundant events has been significantly reduced. “Before ArcSight, we were receiving 550 million events per week from our security systems across the enterprise,” says Troeder. “Due to the intelligent aggregation and correlation capabilities of ArcSight ESM, our security events have been reduced from 550 million per week to just 50,000 – for an incredible efficiency increase of 11,000 to one. That’s a one million-percent improvement!”

Before deploying ArcSight ESM, Vodafone was dedicating a very large percentage of its human IT and computer resources to manually analyze and filter out all of the real events of interest. The company can now handle this dramatically reduced number of events with a much smaller team of well-trained security analysts. Besides the tremendous savings in resources and time, Vodafone has also seen a massive improvement in security. “With ArcSight technology, our highly qualified security analysts can now focus directly on just the real threats. They are no longer wasting time separating the wheat from the chaff,” says Troeder.

ArcSight Professional Services supported Vodafone with the design and deployment of the ArcSight infrastructure. The main focus of the engagement was to help Vodafone enhance its already strong security operations organization. “Even with our massive, complex infrastructure, the ArcSight professional services team helped us to achieve tangible results from our ArcSight implementation in a very short time frame,” says Troeder. Vodafone is now extending its ArcSight footprint to connect more of its security devices deployed in the different Vodafone datacenters and customer services locations around the globe. “With the ArcSight ETRM platform, we not only have an effective solution that enables us to accomplish our near-term goals – it also provides the easy scalability we will need to meet our future requirements as well,” concludes Troeder.

Learn more at hpenterprisesecurity.com

© 2014 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

January 2014

This is an HP Indigo digital print.

HP Restricted: Internal Only