Case study

# du secures network resources, optimizes organizational efficiency, and enables growth

## UAE telecom operator analyzes operations with a complete security information & event management solution

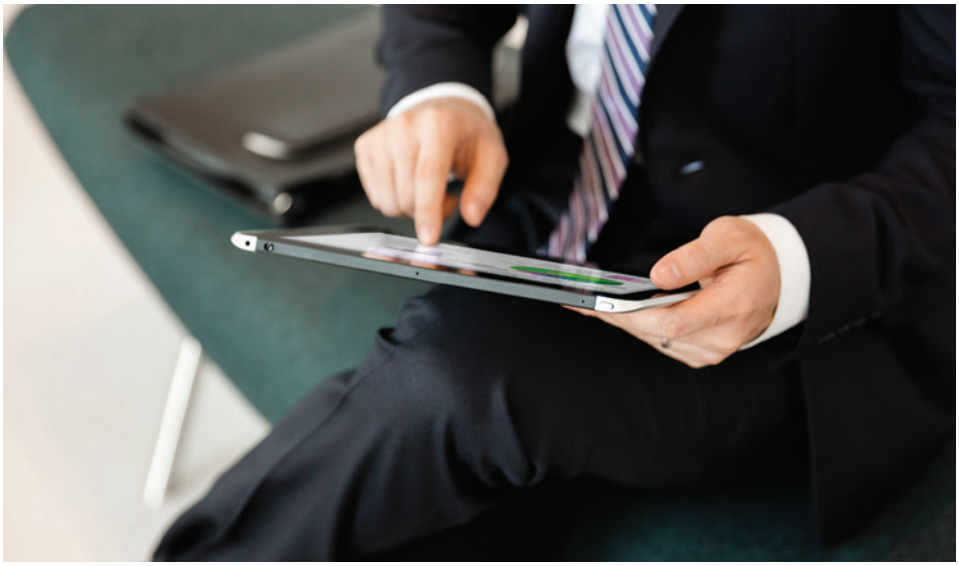
**Industry**
Telecommunications services

**Objective**
Automate security and compliance monitoring to protect network resources, improve operating efficiency, and support the scalable growth of consumer and business services

**Approach**
Implement HP ArcSight Enterprise Security Manager to collect, correlate, and report on security information in real time

**IT matters**
- The development of over 550 intelligence use cases provides true visibility into critical events
- 1,500 log sources are now analyzed in real time
- The Security Operations Center has used the FlexConnector SDK to capture logs from 62 custom device types

**Business matters**
- Security alarm rates reduced by 85%
- The average time to handle a security alert reduced from 24 hours to less than 90 minutes
- 82% of compromise attempts are detected and responded to in less than 24 hours
- Analysis of over 30,000 EPS and development of custom correlation rules to optimize IT efficiency



**"By implementing the ArcSight SIEM solution, we've been able to not only improve operational efficiency but also reduce our security and situational awareness expenditures by about 85% over the last three years."**

– Marwan Bindalmook, Senior Vice President of Technology Security and Risk Management

As a rapidly growing mobile and fixed line service provider, du was faced with protecting its growing network and IT infrastructure while controlling costs and efficiently managing IT operations. By deploying HP ArcSight Enterprise Security Manager, du has been able to automate security and compliance monitoring to cost-effectively support corporate growth while improving efficiency and transforming Big Data into actionable intelligence.

As a company's size and reliance on technology increases, so does the volume of logs it needs to collect, store, and analyze. This has been the case for du, which generates terabytes of security, network, operating system, database, and application log data each quarter. Emirates Integrated Telecommunications Company (EITC) is a telecommunications operator in the United Arab Emirates (UAE) that is commercially branded as du. It offers mobile and fixed telephony, broadband connectivity, and IPTV services to individuals, homes, and businesses throughout the UAE. The company also provides carrier services for businesses and satellite uplink and downlink services for TV broadcasters.

Since its inception, du has consistently maintained a challenging strategic roadmap of supporting sustainable security initiatives. The company also established a Technology Security and Risk Management (TSRM) organization to ensure that du would be able to maintain its leading edge not only in providing superior security initiatives internally, but also in extending its best practices to support the delivery of managed security services.

TSRM set up a Security Operations Center (SOC) with a Security Incident Response Team (SIRT) in 2008. The core of du's SOC is a Security Information and Event Management (SIEM) solution from HP. With over six years of maturity, du is now involved in setting up SOCs as well as offering managed SOC services for enterprises and government institutions throughout the UAE.

## Building scalable SOC infrastructure

As du began building out its SOC, it evaluated best-of-breed products to secure its IT infrastructure. The company selected HP TippingPoint Intrusion Prevention Systems to improve visibility into network traffic and benefit from real-time intrusion protection. TippingPoint platforms were deployed in-line in 2008 to protect du from cyber threats targeting applications, networks, and critical data. "We immediately gained detailed visibility into security threats that help us continuously remain aware of online risks and protect against fraud, viruses, and malware," said Marwan Bindalmook, Senior Vice President of Technology Security and Risk Management for du.

The next step was to replace a SIEM solution that lacked the performance and scalability necessary to support du's business objectives. "We needed to secure fast-growing infrastructure, and that meant our SOC needed the ability to collect, correlate, and report on security information from a diverse range of devices and applications, including security devices, database management systems, and telecommunications equipment," Bindalmook explained. "Our data volumes were exploding, and we needed a higher-performance SIEM solution that could scale with our business growth and provide timely and relevant intelligence to help us quickly detect and respond to any security breaches."

After a careful evaluation, du selected HP ArcSight Enterprise Security Manager (ESM), which provides a Big Data analytics approach to security, transforming Big Data into actionable intelligence that can reduce the costs of a breach and help minimize risk to a business. Using device and application connectors, ArcSight ESM provides a central point for the analysis of daily operations.

Armed with all this data, the real-time correlation capabilities of ArcSight ESM can detect unusual or unauthorized activities as they occur. The visualization and reporting capabilities of ArcSight ESM support dashboards and on-demand or scheduled reports for the SOC team. ArcSight ESM is designed to efficiently store and analyze large volumes of log data. This universal log management solution efficiently collects and stores machine data from any log-generating source and unifies the data for searching, indexing, reporting, analysis, and retention.

## Developing customized use cases

In addition to the out-of-the-box use cases profiling threat conditions that are available with ArcSight ESM, du continuously develops and refines use cases to identify threats. ArcSight ESM is used to identify the relevance of any given event by placing it within the context of who, what, where, when, and why that event occurred, and it assesses the impact of a threat on business risks. It also provides the real-time monitoring, historic analysis, and automated response necessary to manage higher-level business risk events. The organization has now developed over 550 custom use cases based on its business and risk profiling methods.

A comprehensive security management program typically develops and matures over time, and du has been using ArcSight ESM for the last six years. The architecture, packaging, and out-of-the-box features of ArcSight ESM meant that the solution is uniquely capable of scaling both from capacity and feature perspectives and it could meet du's logging, monitoring, and analysis needs with a single solution.

The du infrastructure continues to grow, and ArcSight ESM scales to support the growing needs of the company. The SOC is currently leveraging ArcSight ESM to collect more than 30,000 Events Per Second (EPS) and submits about 5,000 EPS for correlation.

ArcSight's logging format, Common Event Format (CEF) has become the de-facto logging format for almost all device vendors, and out-of-the-box ArcSight ESM supports hundreds of products and its ecosystem is still growing. Using ArcSight's FlexConnector SDK, members of the SOC team develop custom connectors. "We've already developed 62 custom connectors using the FlexConnector SDK," said Tamer El Bahey, Senior Director of Security Monitoring and Operations for du. "It takes a single developer only about two weeks to build a new connector, and we consider the FlexConnector SDK a major advantage because of the diversity of devices it allows us to capture event information from in real time."

## Accelerating resolutions with fewer resources

ArcSight ESM is helping du improve operational efficiency through the automation of manual tasks and optimizing staff efficiency. Successful threat mitigation depends on being able to quickly identify the critical incidents so that they can be handled before they can cause a major negative impact. Reduction in the critical incident rate was crucial for SIRT to effectively respond to incidents. ArcSight ESM helps du filter out the incidents that were resulting in high IT and business risks and act on them more effectively.

Before the deployment of ArcSight ESM, du had to analyze 7,000 alerts per month. As a result, a sizeable security team was required to process the alerts. To help bring the critical event volume under control, du used ArcSight's correlation and rule-building framework to optimize its security alerts. With the appropriate correlation rules and alerts, ArcSight ESM was able to remove false positives and redundant alerts.

TSRM was able to create over 550 custom correlation rules that analyze about 30,000 EPS received in real time from about 1,500 log sources. According to El Bahey, "Three years ago we had 72 correlation rules and now we have over 550. ArcSight makes it easy to create custom rules, we've written them all internally and they allow us to dramatically improve our workforce productivity."

TSRM has also created more than 30 customized filters to parse events from non-traditional IT solutions and telecommunications equipment to gain increased visibility. ArcSight ESM has helped du to gain the threat visibility it needs by increasing the percentage of its incident-to-true positive value by more than 400%.

By fine-tuning the priorities of critical events, security analysts can see the most important items first and the SOC can provide better service levels. The SOC has been able to reduce the security alerts that need analysis from over 7,000 per month to fewer than 1,000 per month, a decrease of over 85%.

## Preparing for the future

"We now have a full-fledged SOC, of which ArcSight is the core element," said El Bahey. "ArcSight helps bridge the gap between business risk and IT risk while improving situational awareness and providing better incident response."

The company continues to improve operations. Now, 82% of compromise attempts are detected in less than 24 hours. The du infrastructure continues to scale; ArcSight EMS analyzed 1,300 log sources last year and now analyzes 1,500 log sources.

## Customer at a glance

**HP Products**

- HP ArcSight Enterprise Security Manager
- HP TippingPoint

While selecting a replacement SIEM solution, a primary TSRM concern was demonstrating how IT-related security risk related to business risks. Though du had purchased multiple best-of-breed security technologies, TSRM found that its original approach of managing logs in their native formats was not delivering the desired results. "By replacing our original SIEM platform with ArcSight, we've been able to integrate logs from diverse technologies under a single umbrella and use ArcSight's powerful correlation engine to develop threat management and risk management use cases to deliver greater value to the business," Bindalmook explained.

The SIEM solution plays a major role in providing SOC and SIRT services internally. "ArcSight helps us to closely align business and IT risks, and today any security initiative, regardless of security technology or security service, must be aligned with the objectives of the SOC," Bindalmook stated. "This helps us maintain the overall objectives of TSRM as well as our Service Level Agreements (SLAs) with business users."

As a result of setting up a world-class SOC with ArcSight ESM at its core, du is starting to offer managed SOC services by setting up of SOCs for enterprises and government customers throughout the region. By leveraging best practices and custom rules and use cases that have been developed and evolved internally, du is extending an internal security initiative into a premium service offering. In this manner, TSRM is evolving from a cost center into a profit center through its advanced implementation of this SIEM solution.

## About du

As a telecommunications service provider in the United Arab Emirate, du has more than 6.5 million mobile customers and almost 50% market share. Over 555,000 fixed line subscribers, 180,000 home services subscribers, and over 70,000 businesses have chosen to use services from du. In a survey conducted by ARC Chart, du was named the Best Mobile Broadband Network in the Middle East and Africa region.

**Learn more at**
**hpenterprisesecurity.com**



4AA5-4723ENW, August 2014