CASE STUDY

Using SGBox, Esprinet anticipates and prevents threats

Company
Esprinet S.p.A.

Sector
Distribution

Implementation
Log Management, Correlation Engine and System Monitoring

Objectives
- Unified platform for diverse handling of information gathered
- Alarm messaging in real time
- Correlation Intelligence

"We believe we are very good at our job. This is why my team of system engineers and I always pay close attention to any market solutions which might help to improve the company's service at global level. It is our aim to maintain the highest level of quality of service which, as the IT team, should always be at least 100%".

Cesare Pedrazzini - IT Manager of Esprinet

Esprinet (Borsa Italiana: PRT), is a leading Italian company and one of the top five in Europe engaged in wholesale distribution of IT and consumer electronics. It has chosen SG Box to ensure robust, versatile monitoring of all its company systems. Esprinet's turnover in 2015 was €2.7 billion and it has around 40,000 client resellers and a portfolio of approximately 600 brands. With a unique internet-based industry sales model, the company focuses particularly on technology distribution to resellers serving small and medium-sized enterprises.

Challenge

In order to check the availability of its services and to gather information from devices and systems, Esprinet used to use different types of software, each with its own system of management. To simplify the process of management of information and alarms detected by different products, it decided to adopt new technology which was more efficient and performed better than that which they were then using. This technology is able to provide an overview and a single check of security problems. This was a matter of priority for Esprinet as they wished to resolve speedily problems relating to systems control. As a pioneer in the IT market, the company therefore decided that now was the moment for adopting new, more efficient technology compared to that previously used.

The solution adopted

Esprinet has adopted and integrated almost all SG Box's modules within its own systems. The LM module (Log Manager) natively supports the standard Syslog and is designed to gather logs of any format and from any source of information. This enables the user to aggregate freely logs from all the company's existing platforms. It is thus possible to analyse the logs gathered, starting with an overview and then delving into the detail so that the individual event can be analysed. This means that the user can, starting with the usage statistic of a resource, reach the point of being able to analyse each individual event which caused it. The LCE module (Log Correlation Engine) is the heart of the platform and allows logs originating from internal checks to be aggregated with those from any source of information within the network and to set up sequences of events in order to identify attacks and other potentially dangerous threats. With the SM module (Security Monitoring) it is possible to check the entire network infrastructure, highlighting potential problems before they occur or recognising them immediately when they do occur. Carrying out continuous monitoring of servers, network devices and services, helps companies to identify and resolve problems linked to the IT infrastructure before they can cause damage to business processes. Finally, there is the SCM module (Security Control Manager), the unified management console, which is designed to manage all the platform modules with features such as advanced reporting and asset management.

> ***"SGBox immediately seemed to us the ideal choice to replace the previous solutions which were covering different problems but with limited functions and high costs in terms of managing different products. After the test phase, we were convinced that we had made the right choice, thanks to the solution's innate versatility. We must take preventive measures to maintain Esprinet's high standards, which have always been recognised by the markets."***
>
> **Cesare Pedrazzini -** IT Manager of Esprinet

Advantages and Results

By adopting SGBox, Esprinet has gained important advantages including the possibility of prompt intervention as soon as a problem is encountered and preventing potential risks.

For example, after a certain number of failed VPN access attempts, the company can intervene, replacing obsolete tokens, with soft tokens. This avoids problems arising with anticipating an event for the user who is blocked from access to the network. Furthermore, by customising ad hoc, Esprinet is able to receive a flow of "live" logs of events which are flagged with warning/ critical notices. All company monitoring not notified by email in real time is displayed to show weaknesses or to predict events.

Future Developments

In anticipation of using other SGBox features within its own information system, Esprinet has also already adopted the NVS (Network Vulnerability Scanner) module which allows the company to undertake scans, which can also be in continuous mode, to ascertain the level of vulnerability of the assets on the network in order to avoid exposure to attacks. This module can also be utilised for auditing configurations, patch and compliance and will contribute to increasing the security of the company network, offering an even better service to its own customers.