



SHELL CONTROL BOX CASE STUDY

IMPROVED INCIDENT MANAGEMENT AT LEADING NETWORK PROVIDER

"THE BALABIT SCB IS AN EXCELLENT SECURITY SOLUTION. IT PROVIDES A LOT OF USEFUL FUNCTIONS WHICH CAN MINIMIZE OUR INCIDENT REACTION TIME."

Senior Security Engineer of the provider

One of the most prominent broadband network services providers in Southern Europe, the customer operates a state-of-the-art fiber-optic network and public cloud infrastructure. Its network consists of a submarine backbone and a terrestrial network connecting major European locations. The customer offers cloud services throughout the region from its privately owned data centers.

THE CHALLENGE

Comply with regulations for cloud providers

As a leading datacenter and cloud services provider, the company must provide its customers with a secure computing environment as well as fulfilling ISO27001 requirements and a number of local security regulations and laws.

Improved monitoring of administrative activities

To meet these criteria, the access to sensitive datacenter systems must be tightly controlled and monitored. The company used log collection and analysis tools before, however logs did not show the result of administrators' command executions. Consequently, to follow the best security practices, the latest standards, and to meet local regulations, the company decided to implement a session-recording solution.

The provider's technical expectations included:



the ability to easily "replay" administrative sessions via an easy-to-use GUI,



the ability to detect malicious activities of third-party administrators and



the improvement of its Incident Management Procedure by quickly detecting, investigating and responding to future incidents.

THE SOLUTION

Turnkey activity monitoring appliance

To meet the above requirements, the provider chose the Balabit's Shell Control Box (SCB) privileged activity monitoring solution. As SCB is a network appliance, it promised fast deployment and low operational costs.

"While other solutions require software agents to be installed on the target servers (and thus possibly modify the server configuration), SCB is an independent device which can be installed quickly and flexibly. And all administrative sessions can be routed via it." – says the Senior Security Engineer of the company.

Multiprotocol solution with "4-eyes" authorization

Among others, SCB was selected for its ability to record the sessions of several different protocols (most notably, SSH, HTTPS, RDP and Telnet), which are all used by the provider's Engineering Team.

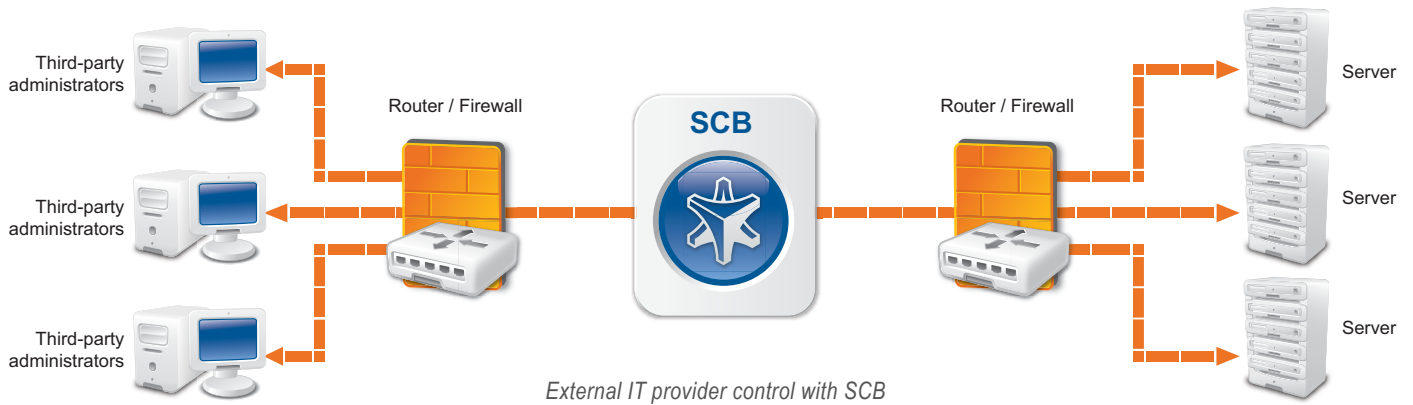
The provider configured the "4-eyes" authorization function of SCB which provides highly controlled access conditions to critical systems. The "4-eyes" allows the external Engineering Team to access systems only when their actions are monitored in real-time by a Security Team member.



Monitor administrators in heterogeneous environment

The SCB was deployed in transparent router mode. Using appropriate routing policies, the Security Team is now able to analyze administrative sessions in three different subnets. The systems that are currently protected by SCB include Windows 2008 & 2012 Servers, Linux servers, Cisco switches, routers and firewalls. In the current configuration, SCB protects 40-50 servers and networking devices and controls 10 concurrent administrative connections in the same time.

“The BalaBit support services were excellent during the initial project phase. BalaBit engineers helped us in making the best decisions on the SCB deployment. They identified the best architecture that fulfil our requirements while keeping all advantages that SCB provides.” – adds the Senior Security Engineer.



BENEFITS

As SCB is a network appliance, its deployment was fast and easy. Implementing SCB resulted in the following benefits for the provider:

- Easy compliance to specific local regulations and international standard requirements,
- Comprehensive and transparent control of third-party system engineers,
- Tighter control of configuration changes in critical systems,
- Lower IT troubleshooting costs and
- Reduced response time to human security incidents.

“THE BALABIT SCB IS AN EXCELLENT SECURITY SOLUTION. IT PROVIDES A LOT OF USEFUL FUNCTIONS WHICH CAN MINIMIZE OUR INCIDENT REACTION TIME. THE PRODUCT SUPPORT AND UPDATES ARE ALSO SUPERB.” – concludes the Senior Security Engineer.

■ [Read more about Shell Control Box](#)

■ [Request online demo](#)

■ [Request callback](#)

ABOUT BALABIT

BalaBit IT Security is an innovative information security company, a global leader in the development of privileged activity monitoring and log management to help protect customers against internal and external threats and meet security and compliance regulations. BalaBit is known for its open source log management application, syslog-ng, which has more than 1 million users worldwide.

www.balabit.com