

EVENT LOG MANAGER



OBJECTIVE: Effectively manage the massive flow of data from different sources.

Employees of a company connect to multiple devices on the internal network, either remotely or in the office. But how do you know if an employee of the organization has his account hacked into and his computer is connecting from a foreign country while he is physically in front of your office?

BLËSK Event Log Manager (ELM) can quickly identify suspicious events from the syslogs it receives. Event Log Manager is a flexible and powerful tool that can store billions of log events, filter through intelligent searching and create tables to better visualize the data. ELM can provide more information as needed.

With ELM's Open Sources tools such as Elasticsearch, Logstash and Kibana, Administrators can be informed immediately of a potential security breach.

BENEFITS

- Creation of dashboards, tables, etc.
- Perform and combine many types of searches – structured, unstructured, geo, metric.

- Zoom out to explore trends and patterns in your data.
- Accepts data of all shapes, sizes and sources.
- Analyze and transform your data quickly.

BLËSK CAN HELP YOU:

It is difficult and uninteresting for an IT team to check all the logs of each machine. However, syslogs are extremely important when a device is hacked or has problems. The mass of Logs collected from different machines must be classified in such a way that they are easy to interpret, so as to avoid making mistakes by manually searching the data.

BLËSK has colorful, easy-to-interpret predefined tables with useful drill-down features to help you find the information you need.

When you click on a particular problem, the graphs change to show only the information related to what you are looking for.

