The OWASP Logging Project

Marc Chisinevski

Digiplug, France

`marc.chisinevski@gmail.com`

The presentation explained current shortcomings of Security Information Management systems. A new solution and a working prototype were presented.

In the current Security Information Management Systems it is difficult to obtain relevant views of consolidated data (for instance alarms concerning different clients and different Data Centres on different periods of time), the difficult to calculate essential indicators for management (such as risk indicators such as Annual Lost Expectancy for Assets and the Cost effectiveness of proposed safeguards), difficult to compare with historical data and also some severe performance issues.

The proposed solution for these problems is based on the usage of multidimensional database, which presents several advantages, such as presenting risk assessment and safeguard cost-effectiveness scenarios to CFO/CEO and presenting data through different useful views (Client, Asset, Data Center, Time, Geography). The Client view is particularly important for Software-as-a-Service and Cloud providers in order to assess conformity with Service Level Agreements and legal obligations for each customer. The Asset view is essential for management, allowing them to assess the risks for business processes and information.

To achieve this, the raw data acquired by the Security Information Management system (events on servers) needs to be correlated and consolidated. The following facts need to be taken into account when assessing the risk: an asset has an intrinsic value and the asset's value increases if other assets (information, business processes, servers) depend on it. Also, risk indicators are easy to calculate and analyze and it is easier to clearly define aggregation levels, such as raw data (Event, Server) and consolidated data (Alarm (correlated events), Asset, Client, Datacenter, Time, Geography). Reporting queries no longer run on the Security Information Management system's production database, it is possible to analyze the data (Drill-down, roll-up, slice) without writing SQL and to integrate data from different sources.