ALERT LOGIC

DEVELOPING SYSTEM COMPONENTS FOR ANALYZING LARGE VOLUMES OF DATA

Client

Alert Logic is the industry-leading provider of on-demand IT compliance and security solutions. The company’s solutions provide organizations with the easiest way to secure networks and comply with policies and regulations. Headquartered in Houston, Texas, Alert Logic is changing the way IT compliance and security solutions are designed, delivered, and utilized.

Challenge

Reksoft cooperation with Alert Logic started in 2007. In the beginning the company was engaged in developing components for two of Alert Logic’s bestselling systems. Log Manager collects, stores and logs information systems for analysis, while Threat Manager detects cyber-attacks and vulnerabilities.
Alert Logic began to focus more on information security services, which demand daily processing of a large amount of data and generation of regular reports. Threat Manager wasn't designed for this volume of processing and data analysis therefore ceased to correspond to the growing needs of the client. Alert Logic needed a new flexible service to instantly detect vulnerabilities in customers’ corporate networks that would work in real time and perform correlation analysis between different network packages. The ability to extend the list of detected network attacks and individually control this service according to the specific needs of clients was one of Alert Logic’s main requirements. Alert Logic formed a list of requirements for the new service:

- Processing of huge data flow from clients' corporate networks 24/7 in real time;
- Possibility to change filter settings and templates for detecting correlations by yourself Access to expanded statistics on incoming data streams to create new models of attack development and carrying out analysis for existing clients.

Solution

New service was named Next Generation Expert System (NGX). Reksoft team took part in the simultaneous development of several products for this new service. Relsoft experts chose the Erlang language as a main instrument of development to enable the creation of easily distributed systems for processing large volumes of data and to suit the clients’ needs in fail-safety features. The development of NGX began in 2012. Reksoft gathered a team of experts especially for this project to help create the functional core of the system.
Development was conducted in several areas. Firstly, it was necessary to create a reliable system of processing and storage of packages that would allow parallel processing of data to be organized at minimal expense.

Challenge

Alert Logic formed a list of requirements for the new service:

- Processing of huge data flow from clients' corporate networks 24/7 in real time;
- Possibility to change filter settings and templates for detecting correlations by yourself Access to expanded statistics on incoming data streams to create new models of attack development and carrying out analysis for existing clients.
- Introduction of flexible interface for setup of filters
- Embodiment of updates and improvement of system without reset or further involvement of programmers
- Continuous building and optimization of system productivity

Result

- Creation of new service for clients' customer data processing in real time, 24/7
- Client's IT service productivity safety grew three times between 2012 and 2014
- Risk of client data loss while using the service was minimized

Technology
Linux, C/C++, Erlang, Riak, MySQL

Services
Development and support of software, creation of Erlang training centre

Timeframe
2012 – 2014

The distributed document-aligned Riak base, which provided flexible, failsafe and reliable storage of the structured objects, was chosen as a system core.

The second area was to create a unified platform for the development of easy agency appendices to collect the information in a network of clients without non-essential productivity losses. It was vital to collect all network traffic data as fast as possible, transform it to a format suitable for subsequent analysis, and send it to the server, providing delivery reliability. Infrastructure for scheduling data packages, which minimized the overhead costs of sending and receiving them, was created. This made it possible to scale decisions according to the needs of client.

The development of the new service was conducted without essential changes to server infrastructure, which ensured the smooth functioning of other services To perform this task Reksoft team optimized productivity of services at different levels and redesigned certain components.Having examined this area, Reksoft specialists conducted the new project on further support and optimization of all the customer's server platforms.
The expert NGX system focuses first of all on automating the monitoring of client systems. This feature was a completely new addition to Alert Logic's service offering. Thanks to the Reksoft' development, the number of mistakes during risk analysis considerably decreased. This helps Alert Logic system analysts to make quick decisions, and to prevent attacks on the basis of available analytical data, and also to improve systems without use of IT resources.

By 2014, the rate of incoming data per minute had grown by more than 3 times and run about 9 thousand packages of the entering data a minute . Reksoft experts carried out a number of tasks on optimization and speed of data processing , that made it possible to hold a constant stock of productivity in 20% of settlement loading, without resorting to serious equipment costs.

Reksoft carried out several tasks:
- Development of a program core for the NGX solution
- Creation of solution for processing and analyzing data in real time
- Introduction of flexible interface for setup of filters
- Embodiment of updates and improvement of system without reset or further involvement of programmers
- Continuous building and optimization of system productivity

Result

Cooperation with Reksoft allowed Alert Logic to improve its solutions, strengthen its strategy and increase its client base, having offered them more convenient, high-speed tools. The Reksoft team performed deep optimization of all key system components of the system. Such actions had increased the system stability, the need for constant control from developers disappeared and risk of losing end customers' data has been reduced.

The system works 24/7 and processes up to hundreds of Gb of incoming data for each client connection. The current client base is growing rapidly, and already have more than 4000 users. The volume of stored information on the server reaches into petabytes. Processing each incoming data package is known within 15 minutes.

- Creation of new service for clients' customer data processing in real time, 24/7
- Client's IT service productivity safety grew three times between 2012 and 2014
- Risk of client data loss while using the service was minimized

REKSOFT HQ
Parkhomenko pr. 10a, 194156, St.Petersburg, Russia

REKSOFT CIS
Aviakonstruktora Mikoyana street 12, Business Center Linkor, block A, entrance 3, 125252, Moscow, Russia

REKSOFT SCANDINAVIA
Isafjordsgatan, 39B 16440, Kista, Sweden