CYBERQUEST

# CyberQuest for BCR:
# Increased Operational Effectiveness for Three Major Divisions within the Bank

BCR

**BCR'S CASE AT A GLANCE:**

- The need to manage data and events in a consistent manner
- Data resides in various disparate systems
- Cumbersome visibility over incident and security data

**SUMMARY BENEFITS:**

- Full overview on database, networking and operational events
- Time savings and resources optimization: light speed answers on events and investigations
- Decision making support due to industry specific dashboards

## Overview

BCR implemented CyberQuest for overview across three major divisions: Networking, Database and UNIX Systems Administration. CyberQuest is a high performance investigation and visibility tool that gathers and unifies data from all sources and makes it available for analysis, reporting and alerting.

BCR is the leader of the Romanian banking system and a member of Erste Group. BCR Group also includes BCR Bank pentru Locuinte SA, BCR Pensii, Societate de Administrare a Fondurilor de Pensii Private SA, BCR Leasing IFN SA and BCR Chisinau SA.

## Customer Challenges &Requirements

The customer required unification of data from various departments, transparency and visibility into security data and events, with the possibility of preventing incidents and reacting based on documented and integrated data. They also needed to correlate and collect data from various products, to ensure security compliance, full reporting and easy investigation of potential incidents.

This translated into:

•quick access for the support and admin teams to operational data in BCR's infrastructure, to enhance the internal and external user experience

•providing the proper instruments for data collection, analysis and reporting across the monitored infrastructure

• improving the operational and security incident response time

The bank was also looking for a light wheight solution for database log collection that did not affect machine performance.

## The Solution

The customer took full advantage of CyberQuest's ability to customize data gathering flows. This enabled the operational and security teams to correlate data from multiple sites and systems, and allowed them to make critical decisions based on these correlations.

*"CyberQuest provided the data unification we needed across multiple locations, along with the complete visibility and enhanced reporting capabilities we were looking for."*

Mugurel Udroiu,
IT Services Analyst

To meet the customer's resource usage requirements, CyberQuest used its new generation collection tool for gathering, parsing and correlating events from files, therefore taking the burden off the customer's infrastructure.

The solution uses the CISCO event definition dictionary to extract and normalize the information from networking equipment and making it available for quick analysis and real-time reporting. Taking advantage of CyberQuest's filtering mechanism that uses logical operands, reporting targets the sensitive systems within the infrastructure and also offers a broad overview of the whole environment.

## Solution Capabilities

- Data cross-correlation between infrastructure and operational applications
- Advanced event search & filter: correlation between billions of events in seconds
- Detailed reporting over each type of information access / modification
- Smart detailed analysis for each security incident
- User defined real-time alerts for the most specific event requirements, in order to enable immediate measures
- Context sensitive dashboards for rapid decision making among infinite data logs
- Predefined scheduled reports to ensure compliance (ISO 27001, COBIT, FISMA, HIPPA, PCP/DSS, SOX) and optimize the internal team's effort
- Intuitive users interface with advanced options for search, filter and data visualization

### ABOUT NEXTGEN SOFTWARE

Nextgen Software is an agile European technology company that delivers innovative cybersecurity software solutions, with a local team of expert programmers with over 15 years of experience in implementing IT infrastructure management and security solutions. Our solutions ensure full visibility, compliance to international standards and regulations, and powerful analytics that keep your company safe and strong.

## Business Value & Results

Unifying and normalizing security logs from separate infrastructures unifying them from the entire production network and offering a single point of access to all the information

A set of comprehensive reports, dashboards and overview for the customer relevant information

Enhanced decision making capability and decision making support

Data source status for quick overview of machine availability and log output. Automatic alerts in case of downtime.