CYBERQUEST

Knows everything™

CyberQuest for Termoelectrica S.A., Republic of Moldavia:
Security compliance and investigation of personal data related incidents

©2018 nextgen software

TERMOELECTRICA'S CASE AT A GLANCE:

◌ The need to be compliant with current data protection regulations

◌ Data resides in many disparate systems (legacy, open source and commercial)

◌ Limited visibility over incident and security data

Overview

Termoelectrica SA implemented CyberQuest for overview and real-time incident response in case of personal data breaches. 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.

TERMOELECTRICA S.A is the main energy producer and provider in Chisinau and surrounding areas. The company covers more than 7,000 buildings, 1,700 companies, 207,000 apartments in 4,560 blocks.

Customer Challenges & Requirements

Termoelectrica was in the final stage of completing a merger with two other companies. This meant they had separate infrastructures, technologies, security policies and event administration coming from each of the three companies.

The customer required unification of data from various systems, transparency and visibility into security data and events, with the possibility of preventing incidents and react based on documented and integrated data. They also needed to correlate old and new technologies and collect data from both commercial and open source products, to ensure security compliance and easy investigation of personal data related incidents.

SUMMARY BENEFITS:

◌ Full overview on document and information manipulation and physical access

◌ Time savings and resources optimization: light speed answers on events and investigations

◌ Decision making support due to context-sensitive dashboards

The Solution

The customer took full advantage of CyberQuest's ability to customize data gathering flows. This enabled the security team to correlate data between open source and commercial solutions of the same type, legacy and current technology, and allowed them to make decisions based on these correlations.

CyberQuest is a revolutionary Big Data Security Analytics Platform that gathers valuable data from multiple technology sources and empowers users to take actionable, critical decisions in real-time.

Solution Capabilities

- Data cross-correlation between the 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

- Integration with physical security systems and correlation of data logs with real life events

- Intuitive users interface with advanced options for search, filter and data visualization
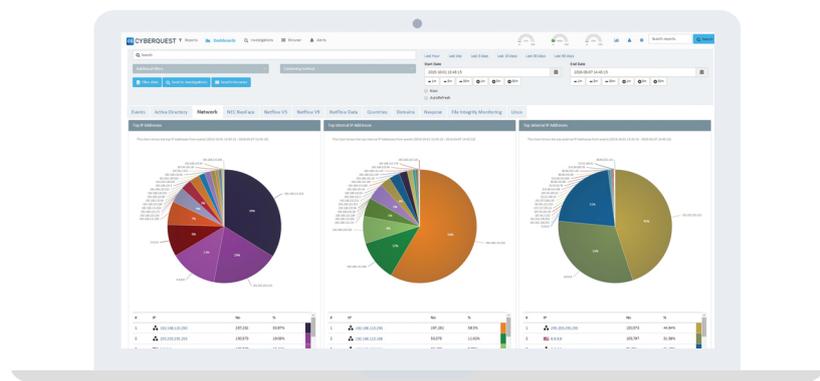
ABOUT NEXTGEN SOFTWARE

Nextgen Software is an agile European technology company that delivers innovative cybersecurity software solutions based on more than 15 years of worldwide experience in successful implementations with both government and enterprise sectors.

Our solutions ensure full visibility, compliance to international standards and regulations, and powerful analytics that keep your company safe and strong.

Business Value & Results

- Policy standardization across the entire environment which supported the merging process of three previously independent companies

- Unifying and defining new security policies for the entire production network

- Unifying and normalizing security logs from separate infrastructures

- A set of comprehensive reports, dashboards and overview for the customer personal data related information

- Technical compliance to current data protection legislation process

- Enhanced decision making capability and decision making support

- Integrating all existing security systems (both physical and virtual)