CQ CYBERQUEST
Knows everything™

CyberQuest ensures the highest level of security investigation for the Romanian National Computer Security Incident Response Team (CERT-RO)

CERT-RO'S CASE:

- The need for real-time threat detection and reaction
- Adoption of the most advanced technologies to face the expansion of increasingly diverse threats

Overview

CERT-RO is the Romanian National Computer Security Incident Response Centre, established in 2011 as an independent organization for the expertise, research and development in the field of cyber infrastructures. CERT-RO is a public institution with legal entity, under the coordination of the Ministery of Communication and the Information Society.

CERT-RO is responsible to prevent, analyse, identify and ensure a timely reaction to cybernetic incidents, meanwhile elaborating and distributing public policies for the prevention and counteraction of incidents that occur within cyber infrastructures.

The Challenge

Considering its high-profile attributions in the national cybersecurity of Romania, CERT-RO seeks to access the latest technologies to counteract the numerous cyber attacks impacting institutions, while creating an active learning framework for public awareness regarding cybersecurity. The need to conduct early-warning detection which leads to real-time defence is vital, given the rise of multiple and sophisticated forms of cyber threats, mostly created with advanced persistent techniques.

SUMMARY BENEFITS:

- Quick time to value: 4-hour deployment
- Time savings and resources optimization: light speed answers on events and investigations
- Decision making support due to industry specific dashboards
- Unlimited built-in horizontal scalability, with no extra database costs

The Solution

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.

CyberQuest collects events from the organization's systems, networks, databases, applications, by using a set of innovative mechanisms, in order to unify and organize data in a coherent format that is easy to follow and analyze.

It operates with very large data volumes, bringing high speed in processing, organizing, accessing and analyzing data – all within seconds – while giving the user the opportunity to efficiently handle the operational flow.

CyberQuest is a No-SQL based application with an advanced new-generation search and filter engine. The navigation across billions of events is made very easily and results are obtained in a

Using its unique self-learning algorithms which ensure full analysis of data flows and the adoption of work patterns for processes, users and systems, CyberQuest sends real-time alerts as it identifies anomalies, augmenting CERT-RO's early warning capabilities and analytics with outstanding intelligence.

A very appreciated solution feature for CERT-RO consisted in the compliance reports, structured according to the latest standards: ISO 27001, COBIT, FISMA, HIPPA, PCP/DSS, SOX.

> Augustin Jianu, General Director, CERT-RO: *"Deploying CyberQuest within our infrastructures offered us the valuable benefit of customization regarding data visibility across multiple platforms and technologies, reporting and early-warning alerts."*

The Results

Implementing CyberQuest brings to organizations the following benefits:

- Context sensitive dashboards for rapid decision making among infinite data logs
- A dedicated search module that returns fast results from the analysis of billions of events in a matter of seconds
- Real-time connectivity to classical SIEM systems for data feeds
- Friendly-user interface with advanced display, search and monitoring functions and customizable filters
- Embedded reports for validating the efficiency of control and compliance processes, work architectures and standards: ISO 27001, COBIT, FISMA, HIPPA, PCI/DSS, SOX
- An innovative real-time alerting system with user-defined alerts that respond to an event's specific needs for ensuring great accuracy and minimum false positives
- The Anomaly Analyzer advanced engine for detecting anomalies
- An interactive and context-sensitive administrative interface (General/Network/Active Directory)

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.