Information Services of Public Institutions Run Safely with a Revolutionary Big Data Security Analytics Platform

AADR'S CASE AT A GLANCE:

- The need to manage key systems of national interest in a secured environment
- Data resides in many systems, with no central visibility and action point

Overview

The Romanian Agency for Digital Agenda (AADR), a public institution within the Ministry for Information Society is managing such information systems of national interest for eGovernance purposes. The Agency's work closely follows the implementation of the Digital Agenda Strategy for Romania with the mission to improve the performance of the public administration and to enhance the citizens' satisfaction.

Among the systems under the Ageny's management, we can mention the following:

- the National Electronic System - SEN (www.e-guvernare.ro)
- the Electronic System for Public Acquisitions, SEAP (www.e-licitaţie.ro)
- the system for the assignment of electronic permits to international road freight transport and the electronic national programs for the assignment of transport routes through the county and inter-county services, SAET (www.autorizatiiauto.ro)
- the national electronic system for the online payment of local taxes, SNEP (www.ghiseul.ro)
- the electronic single contact point (www.edirect.e-guvernare.ro).

The added value of information platforms with direct impact on the activity of a country's public institutions, companies and citizens is perceived and appreciated as long as they are 100% functional, with no interruptions. This is why technical management departments hold a major responsibility for preventing any disruption caused by cyber attacks, human or system errors.

SUMMARY BENEFITS:

- A complete, fully scalable and intuitive solution for IT security investigations and analytics
- 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

Customer Challenges & Requirements

SEAP, the Electronic System for Public Acquisitions is currently one of the most utilised government systems, with over 14,720 public contracting authorities, 56,483 depositor deals and a value of initiated procedures of 345,414,166,938.49 RON in 2014. On the other hand, within the system for assigning road permits, the number of international road transport permits was of 39,714 in 2014, and the number of trucks registered in the system was 31,067. The amount of tax payments without authentication made in the dedicated system in the same year amounted to 21,314,817.15 RON.

Consequently, the responsibility of technical teams overseeing these national wide systems is huge. For collecting, storing and analyzing the large volumes of data, logs and events that are daily operated, AADR installed various SIEM solutions over time, including Dell InTrust, HP ArcSight and AlienVault. After carefully analyzing their activity, the Agency identified the need to implement a unified monitoring solution, one to offer data correlations from a single interface and to improve response times and consequently, the efficiency of IT security officers in case of incidents.

The Solution

After auditing the performance of existing SIEM systems, AADR chose to enhance them with CyberQuest, as it proved to be the most suitable solution to be tested in the Agency's complex cyber environment.

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 currently supervises information flows from the SEN, SEAP, SAET systems and the Virtual Payment Desk, being the one platform through which the Agency's technical department quickly manages security incidents, with a full overview of all vulnerabilities within their data infrastructure.

"CyberQuest is the ultimate security solution. Both reliable and easily approachable by policy makers at all levels, aligned with the latest hi-tech requirements, with a significantly higher responsiveness. All in all, a very comprehensive tool which brings quick problem-solving skills to daily cases managed by our security teams", says Cătălin Gabriel Dumitru, Director of eGovernment Development and Technical Support within AADR.

CyberQuest provides AADR with the necessary capabilities for monitoring the security of their systems and for collecting events from existing SIEMs. The huge amount of collected data is correctly and comprehensively ordered in seconds. This empowers CyberQuest's users to act in real time if the situation requires to.

Based on a No-SQL technology, CyberQuest includes next-generation search features and performance filters, which, by previously defined or ad hoc criteria, help the security officer rapidly investigate security incidents within seconds.

Based on unique learning algorithms, CyberQuest examines collected streams of data to identify patterns of normal work activity, processes, users and systems, so that, afterwards, with the "Anomaly Analyzer" - the dedicated anomaly detection module, to highlight abnormal events and send real-time alerts.

The reporting module is also an essential component of this new security software. CyberQuest generates instant reports in line with the latest industry standards: ISO 27001, COBIT, FISMA, HIPAA, PCP / DSS, SOX.

The investigation, monitoring and reporting modules of CyberQuest are fully integrated into a single, central platform with a user friendly, highly intuitive graphical interface, which uses graphical charts and easy to interpret decision trees to display query results:

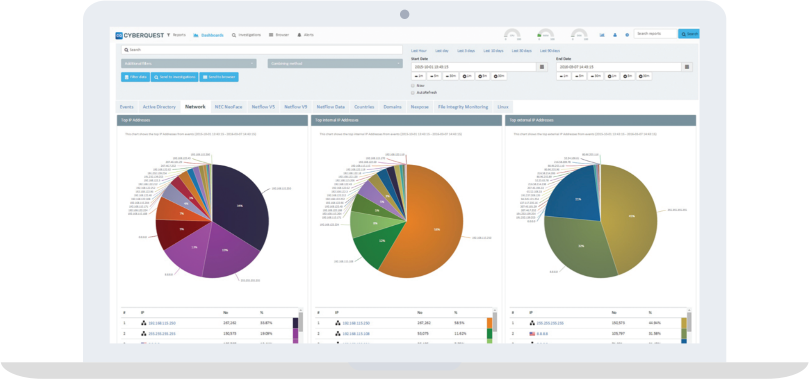
"With CyberQuest, fast and intuitive are the keywords. You get to the desired information with light speed, which leaves you even more time for thorough investigations. This way, you can bring out to the surface vulnerabilities that would be so difficult to identify otherwise. It essentially simplifies the work of our security experts. I can say that at this moment, we finally have a complete technology tool that prevents us from being surprised by security events", added Cătălin Gabriel Dumitru.

> *“ CyberQuest is developed by an astute team of experts and receives the full technical support and logistics of the company, currently a service model in the market in terms of resource management, flexibility and use of the latest available technology. It definitely helps us save time, effort and money, so we can say it’s simply brilliant. We assessed its performance on impressive volumes of data, because this is today’s cyber reality that we must be prepared for.”*
>
> Cătălin Gabriel Dumitru
> Director of eGovernment
> Development and Technical
> Support, AADR

The Results

With CyberQuest, AADR and the public information systems it manages now have a tool that offers:

- Precise identification of security incidents through innovative multi-SIEM / multi-platform data correlation
- A dedicated advanced search module that ensures correlations between tens of millions of events in seconds, therefore saving precious time and resources in the daily work of security managers
- Real-time / schedule-based connectivity to classical SIEM systems for data feeds
- Synthesized results displayed in efficient charts to support the security decision making process
- Context-sensitive interactive dashboards that can be fully customized (General / Network / Active Directory)
- Embedded reports to validate control efficiency and effectiveness for frameworks and standards: ISO 27001, COBIT, FISMA, HIPPA, PCI/DSS, SOX
- An innovative alerting system with real-time, user-defined alerts, which address the most specific event requirements, ensuring great accuracy and minimum false alerts
- Correlations between the Audit Data and Physical Security (using an additional video module)
- A graphical, user-friendly interactive interface, with advanced functions such as: view, search and monitoring through custom filtering



Start Date: 2015-10-01 13:43:15

End Date: 2016-03-07 14:43:15

Top IP Addresses

This chart shows the top IP Addresses from events (2015-10-01 13:43:15 - 2016-03-07 14:43:15)

Top internal IP Addresses

This chart shows the top internal IP Addresses from events (2015-10-01 13:43:15 - 2016-03-07 14:43:15)

Top external IP Addresses

This chart shows the top external IP Addresses from events (2015-10-01 13:43:15 - 2016-03-07 14:43:15)

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.

During the testing sessions of the CyberQuest solution, the Nextgen Software team worked closely with the Agency’s security experts to implement new functionalities and requirements to fit the AADR data infrastructure. The exigent technical requirements of the Agency brought CyberQuest at an even higher level of performance.