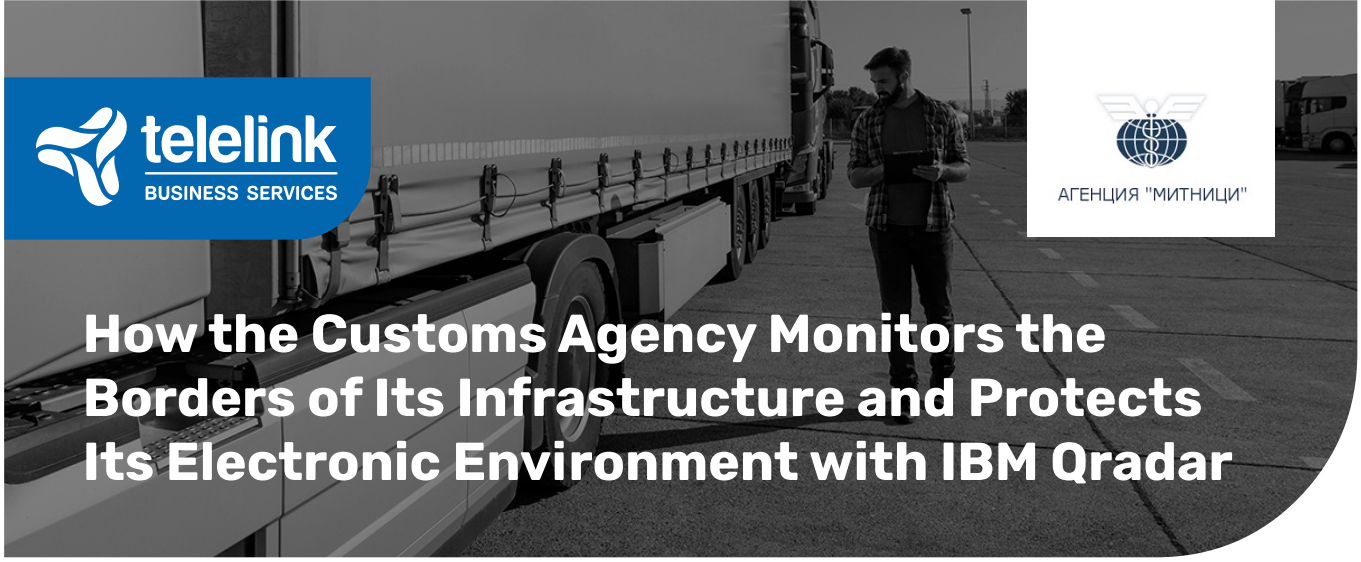

telelink BUSINESS SERVICES

АГЕНЦИЯ "МИТНИЦИ"

How the Customs Agency Monitors the Borders of Its Infrastructure and Protects Its Electronic Environment with IBM Qradar

Protecting society, the environment, and the economy of the country and the European Union. This is the mission of one of the oldest state institutions in Bulgaria – the Bulgarian Customs Administration. And when almost each of its functions today is performed in an electronic environment, it has an equally important and challenging task – to ensure that this environment is secure and any malicious attempts to breach it can be detected and prevented in time. To this end, it needs an automated system for monitoring, analysis, and management of security events (Security Information and Event Management platform or SIEM).

The situation

- Protect a complex digital environment
- Detect malicious attempts and activities early on
- Speed up incident investigations
- Automate analysis and response

The challenging electronic environment

Information technology is a key tool for the Customs Agency in pursuing its vision of greater effectiveness and efficiency as well as seamless integration with EU customs. With the modernization of electronic services and the development of new ones, a number of restrictions in the exchange of documents and information have been removed.

However, the undeniable benefits of digitizing processes also pose risks. If one system is down, even for a short amount of time, this can lead to significant delays in business processes, financial losses, and sanctions, while citizens and businesses may be adversely affected by compromised data. In order to detect potential irregularities and malicious actions in time, an important goal of the Customs Agency and its IT team is to ensure proper and continuous monitoring of the IT infrastructure.

And it is truly a large-scale one. At its center is the Central Customs Administration connected to 130 units through the comprising territorial directorates. All electronic communication with the outside electronic world goes through it. The network, which is served by 400 active network devices, offers 500 Windows- and Linux-based servers running critical services and 3,200 workstations of Agency staff.

THE CHALLENGING ELECTRONIC ENVIRONMENT:

- Large-scale IT infrastructure
- Many and different types of devices
- Numerous sources of security information

Also important for the monitoring are:

- Next-Generation Firewalls
- Email security solutions
- Solutions for analysis of unknown samples of malicious code and suspicious content ("Sandboxing")
- Solutions for endpoint detection and response ("EDR")

The requirements

The Customs Agency's IT team has numerous responsibilities and is looking for a solution with centralized management, which will provide a **comprehensive view of the IT infrastructure entrusted to them**. Among the many requirements for the solution are automation of work processes and independent thorough analysis to **draw attention to the most important events and incidents in real time**, and through appropriate visualizations – to **view and process them easier and faster**. It is also important to automatically detect assets in the IT infrastructure and reveal their vulnerabilities (e.g. missed updates).

With that level of visibility and control, and thanks to the risk assessment of the affected systems, analysts **can purposefully address potential weaknesses**. Heuristic behavior analysis of users covers another aspect of security – for example, internal threats due to compromised access data – allowing the team to **intervene in a timely manner** and limit unauthorized access to information. Last but not least, **in order to improve efficiency and detect irregularities more easily and quickly**, they need integration with additional sources of threat intelligence, on the basis of which to prepare correlation and search rules.

> **Our main challenge is dealing with the tasks at hand with the available resources.**
>
> **Zhelyazko Burlakov,** Head of Department at CA, Department "Network and Information Security Unit"

> **It is very difficult to attract and retain knowledgeable, capable, and dedicated professionals in our field.**
>
> **Krasiyan Andreev,** I-level System Administrator, "Information Systems and Analytics" Directorate, Department "IT Infrastructure Management"

The solution and the approach

Telelink Business Services (TBS) have a solution – IBM QRadar. With years of experience in the integration and management of this SIEM platform, the company's experts are confident in its ability to meet the high requirements. Its functional extensions include QRadar Vulnerability Manager and Risk Manager for Vulnerability Assessment and Risk Analysis, QRadar Behavior Analytics for Behavioral Analysis and IBM X-Force Threat Intelligence as a rich source of threat information.

> **An important advantage of IBM QRadar is the rich features it comes with by default – many supported communication protocols, a long list of supported sources of information and monitoring and correlation rules. All of them can be expanded if necessary. And by scanning the environment and discovering the assets in it, IBM QRadar provides a truly comprehensive view and facilitates decision-making – both in case of an accident and to reduce threats in general.**
>
> **Zhelyazko Burlakov,** Head of Department at CA, Department "Network and Information Security Unit"

The project for integration into the environment of the Customs Agency goes through several phases.

DURING THE FIRST PHASE, a team of TBS engineers examine the IT environment of the Customs Agency, analyzing the network topology and the systems involved. They then create the solution's architecture with the necessary changes to the network infrastructure, defined sources of information, and an integration approach.

THE NEXT STEP is drawing up the complete technical documentation and organizing a training for the Customs Agency's IT team in order to provide all the knowledge necessary for the successful management of the solution.

NEXT, they proceed with the complete integration of IBM QRadar. The purpose of this stage is the physical installation of the solution and its configuration in the environment so that it can collect the necessary information and analyze it. Together, the TBS and Customs Agency teams define nearly 500 rules that will allow the detection of irregularities, taking into account the specific work processes.

AFTER THE FINAL TESTS, the solution is implemented in real operation.

In the process, the TBS team tackles several major challenges that invariably arise in the integration of a SIEM platform. The in-depth analysis of the infrastructure and its detailed description helps the experts identify the important sources of information to be included in the monitoring. During the integration phase, they study the received events in order to develop and improve the detection rules, thus reducing false positives.

The results

The Customs Agency quickly achieves the important benefits it is looking for:

- The team is able to detect attack attempts early on and counteract
- Incident investigation has been accelerated, allowing the team to work effectively
- With the automation of work processes and the optimization of the rules, manual intervention is more of an exception and the overall workload is reduced
- When necessary, the overview of security events can be focused on one system

To Krasiyan Andreev, automation can have an even stronger effect on the work of the Agency's IT team. By implementing SOAR (Security Orchestration and Automated Response) solutions such as IBM Resilient and automating the response, monitoring can lead to effective and instant actions, freeing up valuable time for strategic activities.

However, it is impossible to guarantee that incidents will not happen, especially in a complex environment and a constantly changing world. Therefore, according to Zhelyazko Burlakov and his colleagues, the right approach is to adapt – to know our environment and weaknesses, to assess our capabilities, and to fill in important gaps.

The collaboration between TBS and the Customs Agency continues – they exchange experiences and ideas in the search for the right balance between technology's effectiveness and the experts' ability to make the right, well-thought-out decisions.

It is valuable to have on your side both the technical knowledge and the willingness to share experiences that Telelink Business Services demonstrates every time.

Krasiyan Andreev, I-level System Administrator, "Information Systems and Analytics" Directorate, Department "IT Infrastructure Management"

Telelink Business Services managed the integration process of IBM QRadar and provided us with valuable skills and guidelines to learn how to manage it quickly and fully.

Zhelyazko Burlakov, Head of Department at CA, Department "Network and Information Security Unit"