

Case Study: BH Telecom d.d.



Implementation of Security solutions in BH Telecom

As the leading telecommunications company in BiH, with a large number of users, BH Telecom faces various challenges in terms of security and data protection, applications and devices within the internal infrastructure. Some of these challenges are:

- Protection against unauthorized data access
- Protection against internal attacks and data loss
- How to simplify compliance with regulatory standards (GDPR)
- Identify suspicious attacks and policy violations
- Collecting data relevant to the company's security from various sources such as firewalls, user directories, proxies, applications, routers, etc.
- Insight into the vulnerability of the entire infrastructure and how to protect against them

By implementing appropriate security solutions, our team helps its clients to overcome various security challenges. Within the BH Telecom network, we have implemented the following solutions:

- **IBM Security Guardium** - a solution that offers a centralized set of controls for monitoring real-time database activity, detailed database auditing, automated reporting, database security analysis, DLAC (Data-Level Access Control), automatic detection of sensitive data and many other options.
- **IBM QRadar** - Enterprise solution that combines log traffic data from a large number of devices distributed over the network, makes storage of each data in Raw format, and then does correlation in order to distinguish real threats from fake ones. It offers the ability to record Layer 4 network traffic data in real time, as well as the content of Layer 7 applications, using Deep Packet Inspection technology
- **Qualys Vulnerability Management** - a cloud-based service that provides instant, global visibility where IT systems can be compromised by the latest Internet threats and shows how to protect from them. In this way, it is possible to continuously identify various threats and monitor unexpected changes in the network together with their timely elimination.

The main task and goal was to ensure the integration of these solutions, or better said, enable the review of key information on a single platform, and thus simplify the use of these solutions for the end user.

IBM QRadar was implemented as an umbrella solution that collects information from all segments of the IT infrastructure. Integration with IBM Security Guardium and Qualys VM solutions was performed.

The implementation and integration of these solutions ensured the protection of IT systems and data in the BH Telecom network, as well as enabled timely action on potential threats, malicious data manipulation and remediation of detected vulnerabilities.