LOGPOINT

CUSTOMER CASE

Rapid detection and response to cyber threats

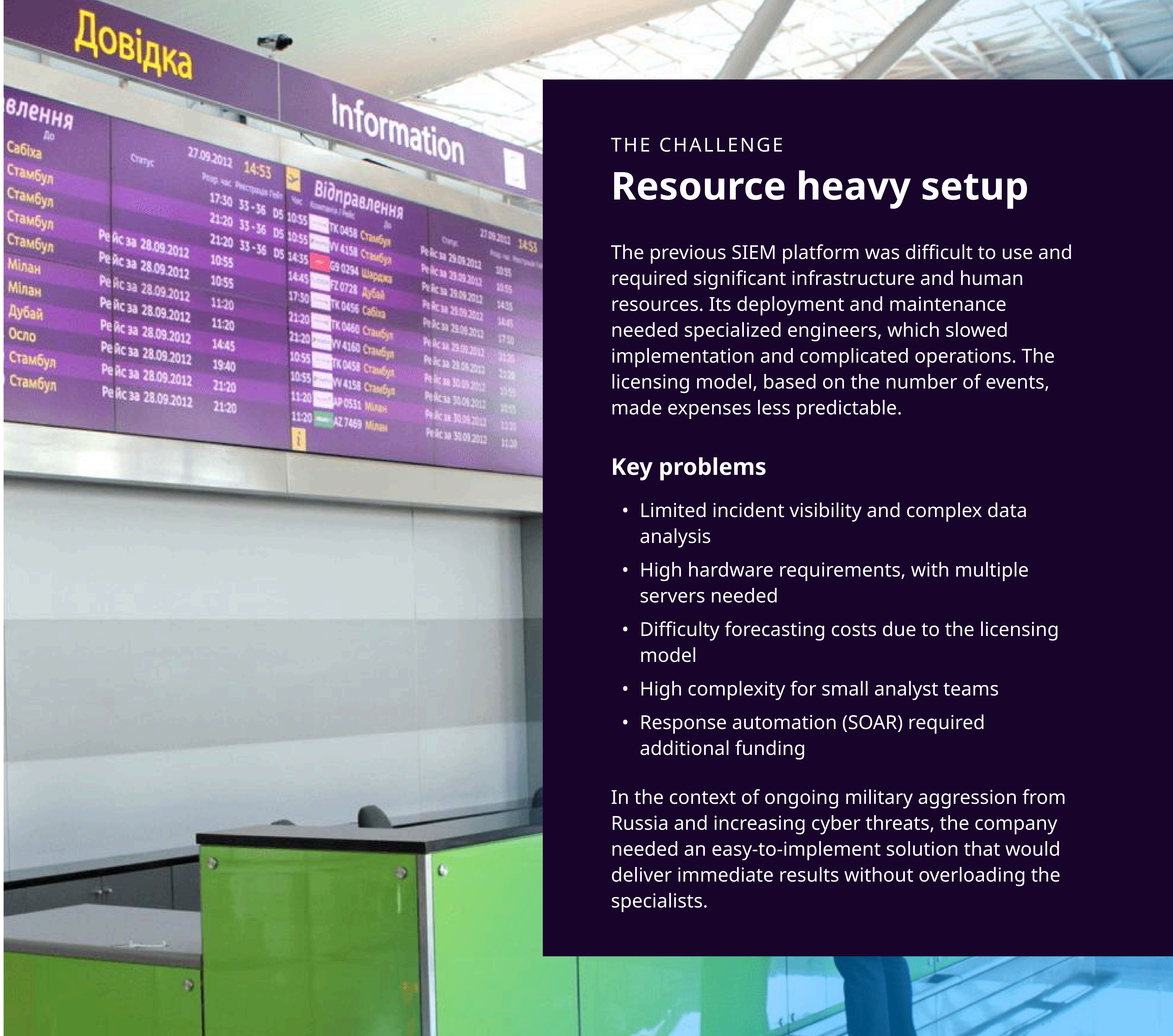
How Boryspil streamlined security operations without overhead

BORYSPIL
INTERNATIONAL AIRPORT

Boryspil Airport

Industry	**Transport, Critical National Infrastructure**
Location	**Kyiv, Ukraine**

Boryspil International Airport is Ukraine's main air gateway and a state-owned enterprise of civil aviation. Before the full-scale invasion, it handled 62% of the national passenger traffic and 85% of cargo traffic. The airport's operational management is based on international standards for passenger service and air transport security. The enterprise has a well-developed IT infrastructure and acts as a provider of digital services, telecommunications, and communications. To ensure stable operations and protection from cyber threats, the information security team required a modern, user-friendly, and efficient cybersecurity system.



THE CHALLENGE

Resource heavy setup

The previous SIEM platform was difficult to use and required significant infrastructure and human resources. Its deployment and maintenance needed specialized engineers, which slowed implementation and complicated operations. The licensing model, based on the number of events, made expenses less predictable.

Key problems

- Limited incident visibility and complex data analysis
- High hardware requirements, with multiple servers needed
- Difficulty forecasting costs due to the licensing model
- High complexity for small analyst teams
- Response automation (SOAR) required additional funding

In the context of ongoing military aggression from Russia and increasing cyber threats, the company needed an easy-to-implement solution that would deliver immediate results without overloading the specialists.

SOLUTION

Seamless rollout for instant value

The choice was made in favor of the Logpoint SIEM solution, which ensured rapid deployment and simple integration of most event sources (logs). During the initial rollout, the majority of event sources were integrated, and the system started working almost immediately — without parser adjustments or additional engineering work.

The basic implementation took about a month, and further configuration was carried out by the company's own specialists after a short Logpoint training.

RESULTS

Faster threat detection and efficiency gain

The shift to Logpoint SIEM enabled the security team to detect and analyze threats faster, optimize workflows, and reduce the load on limited resources. Incidents are now investigated directly from dashboards without the need to run complex search queries.

With a single interface for all critical events, the company increased detection efficiency, reduced response time, and lowered operational costs, freeing resources for strategic tasks.

Main advantages

1. Faster incident detection and response with intuitive dashboards
2. Lower hardware requirements
3. Transparent, predictable licensing for long-term cost control
4. Reduced analyst workload through simpler workflows
5. Future-ready automation with native SOAR capability

BENEFITS

- Single-server deployment
- Node-based licensing, allowing predictable budgeting for years ahead
- Dashboards and analytics out of the box for quick data access
- SOAR readiness, for automated response
- Smooth integration with existing multi-vendor security infrastructure.

> "The Logpoint SIEM solution impressed us with its ease of implementation and use. From day one, all our event sources were integrated into the Logpoint system without extra effort. Its convenient interface and transparent licensing model make it the optimal solution for our team."

Viacheslav Tretiak
Head of Information Security Department,
Boryspil International Airport