

Strengthening National Cybersecurity in the Republic of Moldova with Wazuh



Victor Tataru
Republic of Moldova
Head of Government
Cyber Security

“Wazuh gave us enterprise-level security capabilities with the flexibility and scalability we couldn't afford elsewhere — it's a game-changer for cybersecurity.”

As cyber threats continue to evolve in scale and complexity, government institutions face mounting pressure to secure their critical infrastructure with cost-effective yet comprehensive solutions. In the Republic of Moldova, the Information Technology and Cyber Security Service (ITCSS) plays a vital role in protecting national digital assets. Faced with the need to build a robust and scalable Security Operations Center (SOC), ITCSS turned to Wazuh to meet both operational demands and budgetary limitations.

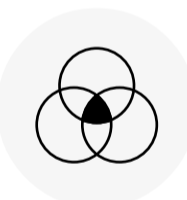
Why Wazuh



OpenSource



Scalability



All-in-one platform

Challenge

Before implementing Wazuh, ITCSS needed a solution capable of delivering complete SOC functionality—event management, access control, user and process monitoring, vulnerability management, CIS compliance, active response, and integration with threat intelligence systems. Most importantly, they required the ability to correlate vast amounts of network and web logs in real time to detect threats and respond swiftly.

The volume of data generated daily—over 5 TB of logs—posed a major challenge. Commercial solutions were not only costly but also limited by restrictive data processing tiers. The agency needed an alternative that could handle enterprise-scale log ingestion and analysis without compromising capability or exceeding their financial capacity.

Solution

Wazuh was chosen for its ability to fully meet these complex requirements in a single, unified platform. Its open-source nature allowed ITCSS to implement and scale the solution across national systems without the licensing restrictions of commercial tools. The platform provided seamless integration with existing infrastructure and offered built-in modules for compliance, active threat response, and advanced log correlation.

By leveraging Wazuh, ITCSS established a centralized, real-time monitoring environment capable of analyzing high volumes of logs and detecting vulnerabilities across multiple systems. Event management and vulnerability management features proved especially valuable in enabling proactive security operations.



Outcome

The impact of Wazuh was immediate and substantial. ITCSS successfully deployed a full-scale SOC capable of defending national infrastructure—most notably ensuring the security of Moldova’s democratic elections during an unprecedented cyber attack. The platform delivered the performance and flexibility required, all within the financial constraints of a public sector budget.

Wazuh’s scalability allowed the organization to continuously adapt and grow its cybersecurity operations without facing additional costs. The team rated their experience with the platform a 5 out of 5, citing its reliability and breadth of features.

Why Wazuh?

The decision to choose Wazuh was driven by three core reasons:

- Open source – Free to use, fully transparent, and adaptable
- Scalability and flexibility – Supports large-scale deployments across national systems
- All-in-one platform – Centralized solution covering all essential security functions

The agency credits Wazuh with enabling a level of cybersecurity maturity that would have otherwise been financially out of reach.

“I just want to thank you for such an important product for global cybersecurity,” they added.