

Executive Summary

EXEO is a cybersecurity-focused organization delivering managed security services across multiple client environments. As its operations expanded, managing and correlating security data across different systems and technologies became increasingly complex.

To address this, the team adopted Wazuh as a centralized SIEM platform. Its open-source model and cost-effective approach allowed them to improve visibility across environments while strengthening compliance capabilities and standardizing monitoring practices.

Challenge

As operations expanded, there were increasing difficulties in managing and correlating security data across multiple environments and technologies. Their infrastructure included a mix of systems, platforms and third-party security tools, each generating its own logs and alerts.

The challenges being faced were:

- Lack of centralized visibility: Security events were distributed across different tools, making monitoring inefficient and time-consuming.
- Complex integrations: Bringing together logs from various solutions required significant effort and lacked standardization.
- Limited correlation capabilities: Without a unified platform, identifying patterns and potential threats across systems was difficult.
- Compliance pressure: Meeting regulatory requirements such as ISO 27001 and GDPR required structured log management, retention, and reporting.

A solution was needed to unify their security operations while remaining flexible enough to adapt to different client environments.

Solution

Wazuh enabled the consolidation of log data and provided real-time visibility across endpoints, servers, cloud environments and third-party tools.

By leveraging custom rules and decoders, detection capabilities were tailored to match specific client environments and compliance requirements. Support for both agent-based and agentless monitoring allowed diverse systems to be integrated without adding operational complexity, creating a more consistent and scalable monitoring approach.



Georges Elias
Managed Security
Services Specialist

"Wazuh has enabled us to centralize, scale, and strengthen cybersecurity operations. By combining flexibility, powerful detection capabilities, and cost efficiency, the platform has become a critical component in delivering high-quality security services and building long-term client trust"

Use Cases



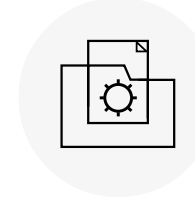
Multi-client security monitoring across heterogeneous environments



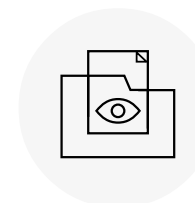
Log aggregation and correlation from multiple security tools



Threat detection (brute-force, password spraying, WAF attacks)



Custom detection rules and decoders



File integrity monitoring



Compliance reporting (ISO 27001, GDPR)



Results

After implementing Wazuh, improvements were seen in both visibility and compliance:

- Full visibility across managed environments.
- Improved correlation and analysis of security events.
- Stronger detection of threats such as brute-force and password spraying attacks.
- More structured compliance monitoring and reporting.
- Standardized security operations across multiple clients.

These improvements allowed the organization to operate with greater consistency while meeting regulatory requirements more efficiently.

Key Benefits

- Open-source platform with strong cost-effectiveness to traditional SIEM solutions.
- Flexible coverage through agent-based and agentless monitoring.
- File Integrity Monitoring (FIM) for real-time detection of unauthorized file changes.
- Unified log collection and correlation from diverse security tools and platforms.
- Compliance support for ISO 27001 and GDPR with audit-ready reporting.

About Exeo

Industry

Managed Services / Cybersecurity

Services

Digital Infrastructure, Managed security services, compliance support and detection engineering, data intelligence.

Location

Europe and Middle East

Company Summary

EXEO is a multi-specialist Managed Services Provider built on three core pillars: EXEO delivers sovereign digital infrastructure, advanced cybersecurity operations, and Data Intelligence services. With its ISO 27001-aligned practices, EXEO helps organisations strengthen their security posture, achieve compliance, and accelerate their digital transformation.