



Executive Summary

DigiFors, a Germany-based Managed Security Service Provider and IT Forensics Specialist, required a scalable and cost-efficient SIEM platform suitable for cloud and on-premise environments. After evaluating various solutions, DigiFors selected Wazuh for its open-source flexibility, scalability and on-premise availability. Wazuh now forms the core of DigiFors' SOC, enabling the company to expand its service portfolio, strengthen customers' IT security posture and reach new market segments.



Stefan Rank-Kunitz
Head of Security Operations Center (SOC).

“Wazuh provides us with a reliable, flexible, and scalable foundation for our managed security services. Its open-source model allows us to deliver enterprise-grade protection while offering tailored solutions for regulated industries”

Challenge

DigiFors supports organizations operating heterogeneous infrastructures across different industries. Customers faced several challenges:


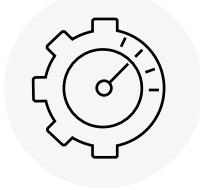
- Distributed systems across cloud, on-premise, and container platforms
- Difficulty correlating security events due to decentralized logs
- Limited real-time visibility into potential threats
- Budget restrictions limiting access to commercial SIEM tools
- Shortage of skilled cybersecurity professionals
- Increasing complexity of cyberattacks
- Severe compliance demands (GDPR, PCI-DSS, HIPAA, NIS2, KRITIS, B3S)

DigiFors needed a unified platform capable of delivering broad visibility, enhancing overall IT security, and enabling efficient SOC operations.

Solution

After assessing multiple alternatives, DigiFors chose Wazuh for its combination of open-source flexibility, scalability, community support, and compatibility with on-premise deployments. DigiFors integrated Wazuh into its SOC and built its security offerings around the platform:

Use Cases

-  Compliance (GDPR, KRITIS, NIS2, PCI-DSS)
-  Vulnerability detection
-  File integrity monitoring
-  Threat detection
-  Incident response

Managed Security Services

- 24/7 SOC monitoring
- Incident response with defined SLAs
- Forensics and complex incident analysis
- Continuous tuning and optimization of Wazuh environments

Consulting & Implementation

- Tailored architectural design and deployment
- Integration with existing infrastructure
- Knowledge transfer and training for customer teams
- Best-practices for long-term operational efficiency

DigiFors also developed customized dashboards, decoders, correlation rules, and industry-specific use cases to address sector-specific security and compliance requirements.



Results

Integrating Wazuh delivered significant value for DigiFors and its customers:

- Strengthened DigiFors’ Managed Security Services portfolio, enabling new service lines centered around SIEM and compliance monitoring.
- Enhanced customers’ threat detection capabilities through centralized log correlation and real-time visibility across heterogeneous IT environments.
- Enabled proactive risk reduction through continuous vulnerability analysis and file integrity monitoring.
- Ensured compliance with KRITIS requirements under the German IT Security Act (§8a BSIG), including automated detection and documentation of reportable incidents within legal timeframes.
- Reduced audit preparation time due to the platform’s automated evidence collection and comprehensive documentation.
- Supported compliance with sector-specific standards such as B3S (water, energy, healthcare) and NIS2 requirements for cyber risk management.
- Improved monitoring of supply chain and third-party access risks, providing customers with reliable regulatory evidence at any time.
- Reduced costs by allowing the decommissioning of other logging solutions.

Additionally, DigiFors leveraged Wazuh’s open-source nature to build custom decoders, correlation rules, and compliance modules, creating differentiated offerings not typically achievable with commercial SIEM products without additional licensing or customization costs. They also implemented a fully automated 24/7 alerting workflow with a structured escalation chain, ensuring rapid incident response. Data sovereignty remains fully with the customer at all times, and the architecture provides high availability with redundant data storage to ensure continuous and reliable operations.

Key Benefits

- Unified SIEM, compliance monitoring, vulnerability detection, and FIM.
- Broad platform support across cloud, on-premise, and container ecosystems.
- Scalable processing for millions of daily events.
- Open-source flexibility enabling custom rules, industry modules, and integrations.
- Competitive pricing with no licensing barriers.
- Seamless integration with SOAR platforms, ticketing systems, and threat intelligence feeds.
- Active community and availability of commercial support options.

About DigiFors

Industry

IT Forensics, Cybersecurity, Managed Security Services.

Services

SOC operations, incident response, forensics, consulting, implementation.

Location

Germany, Austria, Switzerland.

Company Summary

DigiFors provides digital forensics, managed security services and cybersecurity consulting for companies, including those in regulated sectors such as energy, healthcare, and public services.