Wazuh Case Study

iSecNG Strengthening Cybersecurity with Wazuh

iSecNG

Dominik Sigl
iSecNG
Director IT
Security Operations

"Having an customizable open source alternative to closed source SIEMs is in my opinion vital for the security community. Wazuh sucessfully fills this gap."

Why Wazuh

- OpenSource
- Customizable
- Scalability

iSecNG was founded with the mission to provide cost-effective and fair defensive cybersecurity solutions. As regulatory requirements in Germany tightened and businesses sought to improve their security postures, iSecNG needed a robust, scalable, and cost-efficient SIEM and endpoint monitoring solution to support its managed security services. Wazuh emerged as the ideal choice, enabling iSecNG to deliver high-quality security solutions while maintaining cost efficiency and flexibility.

Building a Scalable Security Service with Wazuh

When establishing its service offerings, iSecNG explored various SIEM and security monitoring solutions, including Splunk and Microsoft Sentinel. While these platforms had their own strengths, Wazuh stood out due to three key factors:

- **Scalability:** Wazuh's architecture allows iSecNG to operate a fully scalable environment with multiple clusters tailored to different client needs. Whether managing small 100GB instances or large-scale clusters with multiple terabytes of hot storage, Wazuh ensures smooth operations without performance bottlenecks.
- **Open-source flexibility:** As an open-source solution, Wazuh enables iSecNG to customize configurations, fine-tune detection rules, and tailor security policies to specific client requirements. This level of flexibility is crucial in adapting to evolving threat landscapes.
- **Cost-effectiveness:** Wazuh provides an enterprise-grade SIEM solution at a significantly lower cost compared to commercial alternatives, making it an ideal choice for small and mid-sized businesses looking to strengthen their security without excessive expenditures.

Initially, iSecNG deployed Wazuh using Wazuh Cloud to provide SIEM solutions to its clients. As demand grew, they transitioned to hosting Wazuh in a German datacenter, gaining full control over infrastructure, compliance, and scalability. Today, iSecNG operates multiple Wazuh clusters with high availability (>99.9%), ensuring a secure, reliable, and compliant security monitoring service for its customers.

Meeting Compliance and Security Needs

Many of iSecNG's clients require security solutions to meet regulatory compliance requirements. With the European NIS2 directive approaching, organizations are taking proactive steps to implement endpoint and attack monitoring solutions to avoid potential legal risks. Additionally, businesses seeking ISO 27001 certification must establish a structured approach to security monitoring, where SIEM capabilities are essential.

Achievements

1

Providing a stable and scalable Wazuh cluster based on Kubernetes.

2

Helping small and middle sizes companies all over Germany to increase their security.

3

Close collaboration with Wazuh in terms of partner management, customer success and technical innovation.

Beyond compliance, many companies recognize the need for stronger security and seek expert guidance in implementing an effective SIEM solution. iSecNG provides tailored services to address these challenges, including:

- **Fully managed SIEM services:** Clients receive dedicated Wazuh instances to ensure data separation and regulatory compliance.
- **Managed detection rule services:** Continuous implementation and refinement of detection rules, ensuring accurate threat detection.
- **Managed SOC services:** A 24/7 security operations center that actively monitors, responds to, and mitigates security threats in real time.
- **Wazuh support and consulting:** Assistance with deployment, maintenance, and optimization of Wazuh-based security infrastructures.

By integrating Wazuh, iSecNG helps its clients gain real-time insights into their IT environments, ensuring compliance with regulatory standards while improving their overall security posture.

Delivering Value Through Customization and Open-Source Flexibility

One of Wazuh's greatest strengths is its adaptability to diverse security needs. iSecNG leverages Wazuh's:

- **Lightweight agent**-based data ingestion, ensuring minimal impact on system performance while maintaining efficient data collection.
- **Flexible decoders and rules**, allowing customization to align with specific security requirements and threat landscapes.
- **Active response** mechanisms, enabling automated reactions to detected threats, reducing response times and mitigating security incidents.

While iSecNG utilizes additional Wazuh features such as File Integrity Monitoring (FIM) and Vulnerability Detection, its primary focus remains on delivering a customizable SIEM experience that aligns with each client's unique security needs.
By adopting Wazuh, iSecNG has empowered its customers with enhanced visibility into their IT environments. Clients can now detect security anomalies that previously went unnoticed, reducing risks and improving their ability to respond to emerging threats. The cost-effective model of Wazuh ensures that even small and mid-sized businesses can implement enterprise-grade security without the financial burden of commercial SIEM solutions.

Strengthening Market Position with Wazuh

Since integrating Wazuh into its service offerings, iSecNG has grown into a leading Managed Security Service Provider (MSSP), delivering scalable, compliant, and cost-effective security solutions. Wazuh's flexibility and affordability have enabled iSecNG to expand its customer base while maintaining high service quality and operational efficiency. By leveraging Wazuh's capabilities, iSecNG helps businesses strengthen their security posture, meet regulatory requirements, and enhance threat detection—all while optimizing costs. This partnership continues to fuel iSecNG's growth and solidify its position in the cybersecurity industry.