aa teknoloji

Wazuh SIEM & XDR

Wazuh is an open-source SIEM and XDR platform that boosts cybersecurity strength. It offers a comprehensive monitoring and response solution for IT teams looking to detect threats, meet compliance requirements, and protect endpoints. As a Wazuh Platinum Partner, we deliver end-to-end technical support, deployment, and management services across Europe, Turkey, and the Middle East (MEA). With our regional expertise and robust operational infrastructure, we support organizations' cybersecurity infrastructures at the highest global standards.

Modern Security Challenges

Organizations struggle to provide visibility across distributed IT infrastructures and manage complex cyber threats. Data fragmentation and manual processes delay threat detection while severely reducing the efficiency of cybersecurity operations. Security teams are overwhelmed by isolated log data and reactive response methods. Loss of centralized control over scattered endpoints makes it harder to detect and block threats.
The continuous monitoring and auditability pressure brought by legal regulations such as KVKK and ISO 27001 makes manual management impossible.

⚠ Who can benefit?

- For teams seeking visibility across a distributed IT environment
- For SOC teams overwhelmed by manual log review workloads
- For organizations struggling with KVKK and GDPR compliance processes
- For those wanting to automate vulnerability detection and patch management

Core Principles

Centralized
Combines all data into a single dashboard.

Automated
Detects threats swiftly and automatically.

Unified
Merges SIEM and EDR capabilities.

Compliant
Provides full support for regulatory processes.

How Does Wazuh Works?

Wazuh is a comprehensive security platform developed to detect, analyze, and generate automated responses to cyber threats in your corporate environment. The working logic of the system is built on a three-stage process involving centralized data collection, intelligent correlation analysis, and rapid incident response.

Technical Specifications

Unified Threat Detection
- Performs real-time log correlation
- Monitors endpoint activities
- Provides file integrity control
- Continuously scans critical systems

Compliance and Risk Management
- Offers KVKK and GDPR dashboards
- Creates continuous audit trails
- Automatically identifies vulnerabilities
- Reports security weaknesses

Flexible Deployment Architecture
- Supports on-premise installation
- Compatible with hybrid cloud structures
- Operates in air-gapped environments
- Provides high availability

SOC Operations Support
- Windows, Linux, macOS support
- Integrates with SOAR platforms
- Centralized single-panel monitoring
- Automated response mechanisms

SOC Operations Support
- Windows, Linux, macOS support
- Integrates with SOAR platforms
- Centralized single-panel monitoring
- Automated response mechanisms

Workflow

1. Data Collection
- Collects logs live from endpoints.
- Processes all cloud and physical data.
- Provides continuous monitoring via agents.
- Combines different sources into one.

2. Threat Analysis
- Finds malicious software instantly.
- Continuously audits system files.
- Monitors unauthorized access attempts.
- Searches for anomalies with rule sets.

3. Response and Report
- Executes automated response mechanism.
- Generates reports compliant with regulations.
- Prioritizes security vulnerabilities.
- Transmits instant data to SOC panels.

Continuous Improvement
With high availability and clustering support in on-premise, hybrid, and cloud environments, it grows along with your infrastructure, helping you preserve your strategic security focus by reducing operational burdens.

Advantages

Centralized Security Visibility
Speeds up monitoring and analysis processes by combining data from all endpoints, servers, and cloud applications across distributed IT infrastructures into a single dashboard.

Automated Threat Detection
Reduces the workload of SOC teams by instantly detecting malicious software and unauthorized access attempts through built-in rule sets and advanced threat intelligence.

File Integrity Monitoring (FIM)
Instantly reveals rootkit activities and unauthorized interventions by continuously tracking all changes made to critical system files and registries.

Automated Compliance Auditing
Simplifies legal audit processes with predefined dashboards and automated reporting tools for standards such as KVKK, GDPR, PCI-DSS, and ISO 27001.

aa teknoloji

AA Teknoloji is an AI-powered media technologies platform developed for modern newsrooms. Our integrated solutions, ranging from news workflow systems to digital archive solutions, real-time broadcasting infrastructure to multi-channel content management, accelerate the digital transformation processes of media organizations and offer scalable broadcasting operations.

For more information, visit aateknoloji.tr or follow the @aateknoloji LinkedIn account.