

ESET and Wazuh

Unified security visibility and efficient threat response for your business

Enhancing Cybersecurity with Seamless Integration

Security professionals, such as Security Analysts and IT Administrators, face increasing cybersecurity challenges and require cost-effective solutions to monitor and respond to threats efficiently. Small and medium-sized businesses (SMBs) and enterprises alike must deal with large volumes of security data, incomplete visibility, and limited resources across multiple security consoles. These challenges can lead to delayed threat detection and response, increasing the risk of security breaches and data loss.

ESET's integration with Wazuh provides a unified security platform that consolidates security alerts, telemetry, and incidents into a single pane of glass. This integration enhances the ability of organizations to detect, investigate, and respond to threats more effectively. By leveraging API-based integration, Wazuh can query and pull relevant security events, incidents, and telemetry directly from:

PROTECT PLATFORM

ESET's award-winning endpoint protection platform that offers advanced threat detection and prevention capabilities.

INSPECT

The platform's Extended Detection and Response (XDR) module that provides deep visibility into endpoint activities and advanced threat hunting capabilities.

CLOUD OFFICE SECURITY

ESET's business cloud email and app protection (MS365, Google Workspace) module that safeguards cloud-based email and collaboration tools from malware, phishing, and other threats.

This seamless integration ensures that security teams have a comprehensive view of their security posture, enabling them to correlate endpoint data with network and cloud security information. The unified platform reduces the complexity of managing multiple security solutions, allowing security professionals to focus on proactive threat management and incident response.

KEY BENEFITS

UNIFIED SECURITY VISIBILITY

Consolidate endpoint, network, and cloud security data into a single console for comprehensive threat detection and response.

IMPROVED SECURITY POSTURE

By ingesting high-quality ESET data, organizations will optimize their security posture.

AUTOMATED DATA CORRELATION

Reduce manual overhead and response times with automated data ingestion and correlation.

ENHANCED EFFICIENCY

Security teams can do more with fewer tools and less manual input, improving overall efficiency.

KEY FEATURES

REAL-TIME ALERT STREAMING

Stream ESET endpoint alerts directly to Wazuh in real-time, allowing for immediate correlation with firewall logs, IDS/IPS data, and user activities.

CATEGORIZED DATA

Utilize Wazuh's Rules functionality to categorize ESET logs into existing categories for proper data organization.

AUTOMATED ACTIONS

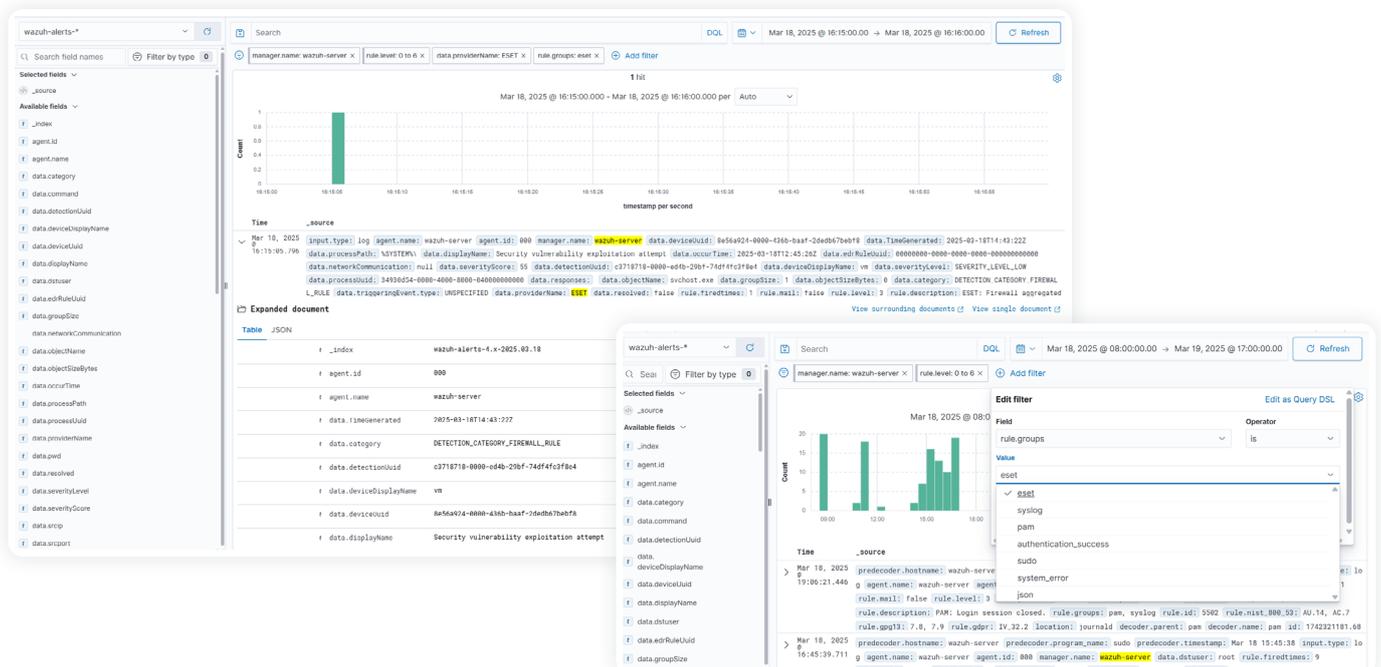
Wazuh's alerting and workflow capabilities can automatically trigger containment and remediation actions on endpoints via ESET's management APIs.

ADVANCED BUSINESS EMAIL AND APP PROTECTION

Ensures that email, the number one threat vector, receives proactive ESET protection that goes beyond inbuilt Microsoft365 and Google Workspace protection.

HOW IT WORKS

The integration works by using REST APIs (HTTPS) for secure queries and data retrieval. Wazuh runs a provided application that queries ESET PROTECT, ESET Inspect, and ESET Cloud Office Security for detections in real time. The data is then made available via PublicAPI for Wazuh, enabling seamless integration and unified security visibility.



About ESET

PROACTIVE DEFENSE. MINIMIZE RISKS WITH PREVENTION.

Experience best-in-class protection thanks to ESET's in-house global cyber threat intelligence, compiled and examined for over 30 years, which drives our extensive R&D network led by industry-acclaimed researchers. ESET PROTECT, our cloud-first XDR cybersecurity platform, combines next-gen prevention, detection, and proactive threat-hunting capabilities. ESET protects your business so you can unlock the full potential of technology.

About Wazuh

Wazuh is an open-source security monitoring and compliance solution that unifies XDR and SIEM capabilities and helps organizations detect and respond to threats efficiently. With a focus on cost-effectiveness and scalability, Wazuh serves both SMBs and enterprises, providing customizable security monitoring across complex infrastructures. Wazuh integrates with various platforms to offer comprehensive visibility and protection, ensuring that security teams can effectively manage and mitigate risks.