Security Events Collection and Analysis

Agent-Based Log Collection

The platform leverages agent-based log collection capabilities, utilizing the Wazuh agent for comprehensive security event monitoring and analysis.

Supported Operating Systems

The Wazuh agent can be deployed on a wide range of operating systems, including:

- Windows
- Linux distributions
- macOS
- FreeBSD
- OpenBSD
- Solaris

For details on supported platforms, refer to the Official Wazuh Agent Documentation.

Flexible Log Collection

The platform offers versatile log collection options:

- Ability to monitor various log file types and formats
- Support for Windows event logs
- Customizable log parsing and formatting

Configurable Log Sources

Administrators can configure the agent to collect logs from:

- System logs
- Application logs
- Custom log files
- Windows event channels

Advanced Features

- Real-time log monitoring and analysis
- File integrity monitoring
- Command output collection
- Centralized configuration management

Scalability

The agent-based approach allows for efficient log collection across large-scale environments, from individual endpoints to enterprise-wide deployments.

By leveraging the Wazuh agent's capabilities, the platform provides a robust foundation for comprehensive security event collection and analysis across diverse IT infrastructures.

Agentless Log Collection (Active Mode)

The platform actively collects logs from devices that do not support agent installation, such as network devices. It uses SSH to connect to devices and execute commands for log and status information retrieval.

Agentless Collection Method

The system utilizes Secure Shell (SSH) protocol to establish secure connections with target devices, enabling remote log and status information retrieval without on-device agents.

Supported Devices

This method is ideal for:

- Network switches and routers
- Firewalls
- Load balancers
- Other network appliances or devices with limited software installation capabilities

Collection Process

- **Secure Connection**: The platform initiates an SSH connection to the target device.
- **Command Execution**: Pre-configured or custom commands are executed on the device.
- **Data Retrieval**: Log data or status information is collected based on command output.

Flexibility

- **Customizable Commands**: Administrators can tailor the commands executed on each device type to collect specific logs or information.
- **Scheduled Collection**: Log retrieval can be automated regularly to ensure up-to-date information.

This agentless approach significantly enhances the platform's ability to provide a holistic view of an organization's security posture, integrating both agent-supported and agentless devices.

Agentless Log Collection (Passive Mode)

The platform offers advanced log processing capabilities with a focus on **syslog protocol integration**. Its architecture is highly flexible and scalable, adapting to various log volume requirements.

Syslog Processing

The system efficiently handles logs transmitted via the syslog protocol, a widely used standard for system logging.

Flexible Ingestion Architecture

Depending on anticipated log volume, the platform can be configured with:

- **Multiple Remote Syslog Servers**: For distributed log collection and processing.
- **Message Bus Systems**: Integration with technologies like Kafka for high-throughput log streaming.

Scalable Design

The platform's architecture is tailored to match expected log volumes, ensuring optimal performance and resource utilization.
This approach enables efficient management of varying loads, from small-scale deployments to enterprise environments with massive log volumes.

Public Cloud Audit Logs Collection

The platform offers comprehensive **audit and management log collection** for major public cloud environments, including **AWS, Google Cloud Platform (GCP), and Microsoft Azure**. This integration allows organizations to centralize and analyze critical operational data from their multi-cloud infrastructures.

- **Multi-Cloud Coverage**: Native support for major cloud providers ensures broad visibility across diverse cloud environments.
- **Audit and Management Focus**: The platform collects security-critical audit and management logs for compliance and operational oversight.
- **Extensible Framework**: Custom integrations can be developed for cloud services not natively supported.
- **Tailored Solutions**: The platform adapts to unique organizational requirements, enabling additional integrations as needed.

By centralizing these critical logs, the platform enhances **cloud governance, security monitoring, and compliance management** across multi-cloud environments.

SaaS Audit Logs Collection

The platform supports **log collection from various SaaS applications**, providing multi-source log integration tailored to client needs.

- **Diverse SaaS Integration**: Collect logs from multiple SaaS services, accommodating various application types and data formats.
- **Customizable Implementation**: Integration is provided on a per-request basis to meet unique client requirements.
- **Flexible Log Collection**: The system handles multiple log types and sources simultaneously for a comprehensive view of an organization’s SaaS ecosystem.
- **Scalable Solution**: As new SaaS applications emerge, the platform can incorporate additional log sources as needed.

This flexible and extensible approach enables **deeper insights into SaaS operations, enhanced security monitoring, and improved operational visibility** across cloud-based services.

Revision #1
Created 30 March 2025 06:04:13 by Bryan
Updated 30 March 2025 06:08:14 by Bryan