

Welcome to SmartObserve: The Next Generation of OpenSearch

SmartObserve is a cutting-edge evolution of OpenSearch by Integrated Global Solutions Limited, enhancing data search and visualization. It offers an open-source solution under the Apache License 2.0. With compatibility with Beats and Logstash, plus advanced plugins, SmartObserve delivers exceptional performance, flexibility, and scalability for all your data needs.

Features



Intuitive Interface -
Sidebar, Dashboard &
Visualization Choices



Central Log Search,
Visualization, & Dashboard



Flexible Log Retention
Policy for all Security Logs



Query Workbench -
Advanced SQL /
Splunk-like queries for
flexible data interrogation



APM - Trace Analytics



Detect and
Alert Security Threats

Benefits

Cost Management

Helps avoid and manage unpredictable cost increases through pre-study arrangements

Cost Elimination Middleware

By pre-engaging in log assessments between the log server and Splunk

Online Dashboard

For real-time monitoring of the status of different devices

Comprehensive Log Coverage

Fully covers security and audit logs across systems, networking, and security domains

Abnormal Activity Monitoring

Monitors security solutions for abnormal activities, including endpoints, NDR, firewalls, AD, and more

Leverage OpenSearch Platform

To analyze, report, and present indicators of security status

Use Cases

General Purpose Search Engine



E-commerce Search

Efficiently search inventory catalogs.



Document Search

Comprehensive document
search capabilities



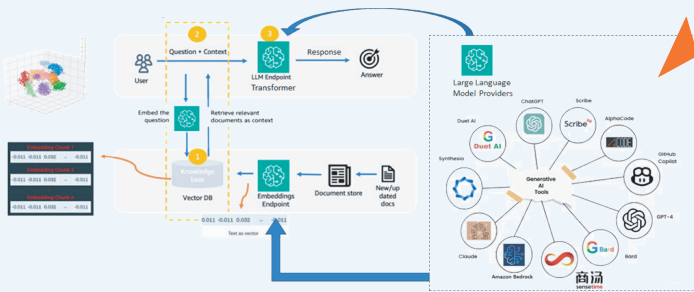
Application Search

Embed search functionality
into applications



Query Offloading

Economical querying without
impacting DBMS performance



Vector Database

Machine Learning Embeddings: Encode documents, images, and audio into vectors.

k-NN Search: Leverage k-nearest neighbors functionality.

RAG Workflow: Support Retrieval Augmented Generation for AI applications.

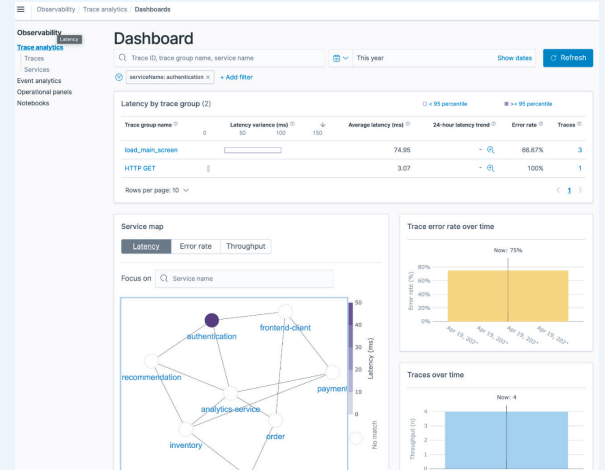
Infrastructure / Application Metric / Log Monitoring

Real-Time Monitoring: Provides real-time dashboards for monitoring the status and performance of various devices and applications.

Service Map Visualization: Visualizes service interactions, highlighting latency, error rates, and throughput.

Trace Analytics: Identifies performance bottlenecks and error patterns over time through detailed trace analysis.

Comprehensive Log Analysis: Enables detailed analysis of logs to detect anomalies, performance issues, and security threats.



Log types and rules

Select a category type you would like to detect

Windows logs (selected)

Detection rules (1582 selected)

Rule name	Rule severity	Log type	Source	Description
Monika Rootkit	Critical	Windows	Custom	Detects the use of Monika rootkit as described in the securisat Operation 'Operational report'
TROJAN DCOM Internet Explorer Application Virtual DLL Hijack	Critical	Windows	Sigma	Detects a threat actor creating a file named 'teruul.dll' in the 'C:\Program Files\Internet Explorer\ directory over the network and loading it from a DCOM Internet Explorer DLL Hijack scenario
Registry Persistence Mechanism via Windows Telemetry	Critical	Windows	Sigma	Detects suspicious method using windows telemetry
CobaltStrike Service Installations in Registry	Critical	Windows	Sigma	Detects known malicious service installs that appear in cases in which a Cobalt Strike beacon executes privileged or lateral movement. We can also catch this by system log 7045 (https://github.com/SigmaHQ/sigma/blob/master/rules/windows/defense/defense_cobaltstrike_services_installs.yml) in some SIEM you can catch those events also in WMI\SystemControlSet\services or WMI\SystemControlSet\services, however, this rule is based on a regular system's events.
Sticky Key Live Backdoor Usage	Critical	Windows	Sigma	Detects the usage and installation of a backdoor that uses an option to register a malicious debugger for both-in-logs that are accessible in the logs stream
Security Support Provider (SSP) Added to LSA Configuration	Critical	Windows	Sigma	Detects the addition of a SSP to the registry. Upon a reboot or API call, SSP DLLs gain access to encrypted and plaintext passwords stored in Windows.

Security Analytics

Abnormal Activity Monitoring: Monitors security solutions for abnormal activities across endpoints, NDR, firewalls, AD, and more.

Open Source Wazuh Platform: Leverages the Wazuh platform to analyze, report, and present indicators of security status.

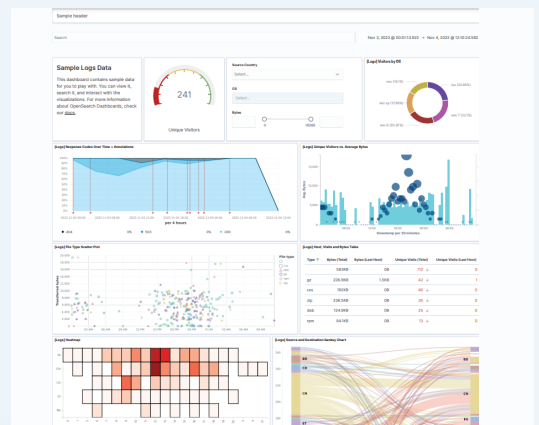
High-Threat Alert Monitoring: Continuously monitors high-threat alerts for in-scope infrastructure components.

Cost Reduction with Data Offloading

Reduce License Costs: Offload data from Elastic or Splunk to reduce expenses.

Data Source Connection: Streamlined data management with SmartObserve Data Offloading Engine.

Efficient Data Management: Handle large data volumes effectively.



Contact us today to learn more about how SmartObserve can benefit your organization.

Contact us

info@igsl-group.com

www.igsl-group.com

Follow us



LinkedIn



Facebook

Integrated Global Solutions Limited