

Welcome to SmartObserve: The Next Generation of OpenSearch

SmartObserve is a cutting-edge evolution of OpenSearch by Magic Creative Software 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



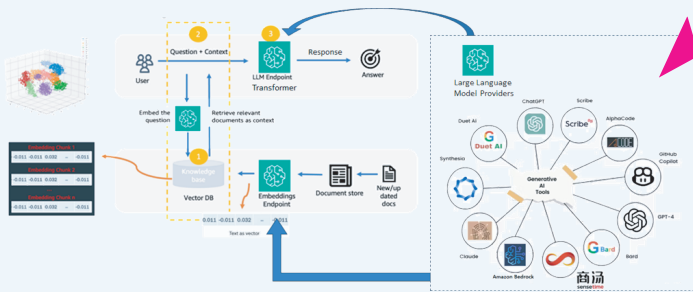
Application Search

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.

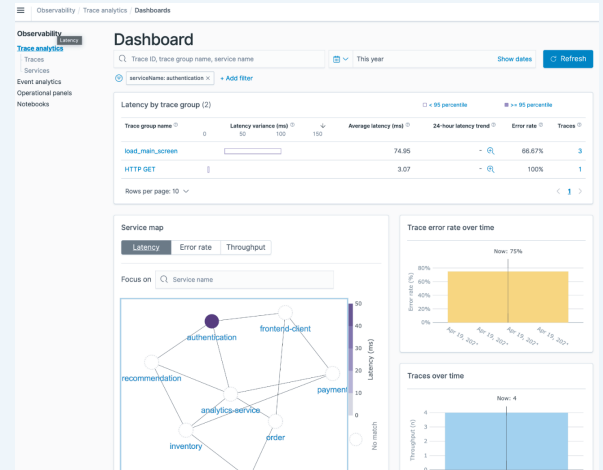
Infrastructure / Application Metric / Log Monitoring

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				
Choose the log types that correspond to your data source. Detection rules are automatically added based on your chosen log types.				
Select a category type you would like to detect				
<input type="radio"/> Netflow	<input type="radio"/> DNS logs	<input type="radio"/> Apache access logs	<input checked="" type="radio"/> Windows logs	
<input type="radio"/> AD/LDAP	<input type="radio"/> System logs	<input type="radio"/> Cloud Trail logs	<input type="radio"/> S3 access logs	
Detection rules (1582 selected)				
Detection rules are automatically added based on your chosen log types. Additionally, you may add or remove detection rules for this detector.				
Q Search...	Rule severity	Log type	Source	Description
<input checked="" type="checkbox"/> Moriya Rootkit	Critical	Windows	Custom	Detects the use of Moriya rootkit as described in the securisid Operation "Sideloaded report"
<input checked="" type="checkbox"/> T1021 DCOM Internet Explorer Application WMI DLL Hijack	Critical	Windows	Sigma	Detects a threat actor creating a file named "teruuts.dll" in the "C:\Program Files\Internet Explorer\" directory over the network and loading it in a DCOM Internet Explorer DLL Hijack scenario.
<input checked="" type="checkbox"/> Registry Persistence Mechanism via Windows Task Scheduler	Critical	Windows	Sigma	Detects persistence method using windows task scheduler
<input checked="" type="checkbox"/> CobaltStrike Service Installation in Registry	Critical	Windows	Sigma	Detects incoming malicious service installs that appear in cases in which a CobaltStrike beacon executes privilege or lateral movement. See also using this log system log T1059 (https://github.com/SigmaHQ/sigma/blob/master/rules/windows/defense/cobaltstrike_service_installs.yml) In some SIEM you can catch those events also in WMI/MSI/Service/ControlService or WMI/MSI/Service/ControlService/Service, however, this rule is based on a regular system's events.
<input checked="" type="checkbox"/> 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 built-in tools that are accessible in the high event.
<input checked="" type="checkbox"/> 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.

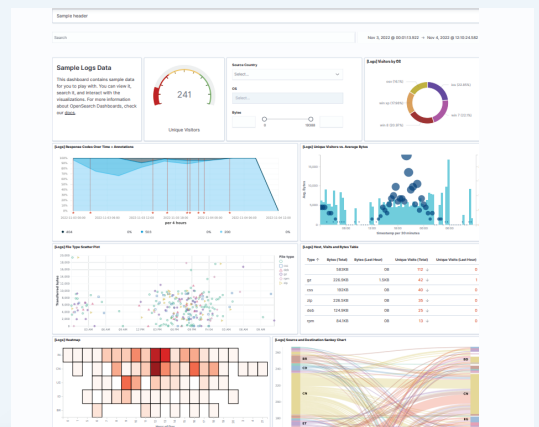
High-Threat Alert Monitoring: Continuously monitors high-threat alerts for in-scope infrastructure components.

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@magiccreative.io

www.magiccreative.io