# OpenSearch as a SIEM Solution

OpenSearch is a scalable open-source search and analytics platform that can serve as the core of a Security Information and Event Management (SIEM) system. OpenSearch can centralize logs from diverse sources, apply detection rules, and generate alerts for suspicious activities.

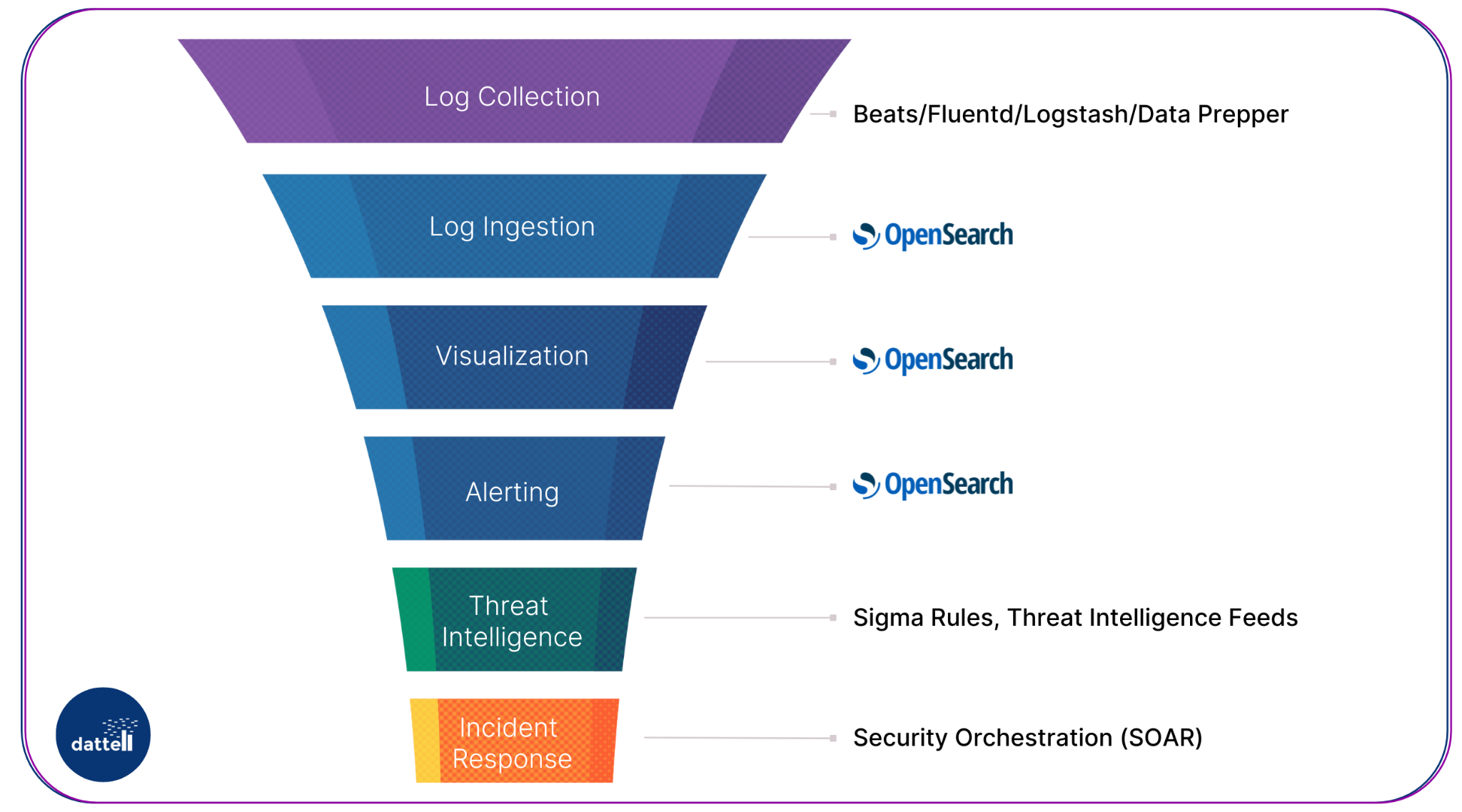


Figure 1. OpenSearch can serve as the core of a SIEM system.

Its built-in [Security Analytics](https://opensearch.org/docs/latest/security-analytics/#:~:text=Security%20Analytics%20is%20a%20security,responding%20effectively%20to%20potential%20threats) package provides SIEM capabilities to investigate, detect, analyze, and address security threats in real-time:

Security Analytics provides an out-of-the-box solution that installs automatically with any OpenSearch distribution. It includes the tools and features necessary for defining detection parameters, generating alerts, and responding effectively to potential threats.[1](https://opensearch.org/docs/latest/security-analytics/#:~:text=Security%20Analytics%20is%20a%20security,responding%20effectively%20to%20potential%20threats)

Below, we discuss how OpenSearch addresses key SIEM use cases – Threat Detection, Log Analysis, and Compliance Monitoring.

## Threat Detection with OpenSearch

The Security Analytics plugin can monitor logs for anomalous activity and detect potential security threats in real-time. And when threats are identified, OpenSearch can trigger alerting.

This workflow from log ingestion to alerting is achieved through a combination of detection rules and automation.

Detectors, Rules, and Anomalies.  
Detectors are used to identify threat patterns in log data. Each detector targets a particular type of log (network logs, authentication logs, etc.) and is mapped to known adversary tactics. OpenSearch leverages the MITRE ATT&CK organization’s collection of “adversary tactics and techniques”.[2](https://attack.mitre.org/)

Threat detection rules define the logic for identifying security incidents. A library of Sigma rules is included with OpenSearch’s Security Analytics package. Two examples of rules are (1) flagging multiple failed logins followed by a successful admin login or (2) identifying the presence of known malicious IP addresses in firewall logs.

OpenSearch can also incorporate anomaly detection using machine learning (via its ML Commons plugin[3](https://opensearch.org/docs/latest/ml-commons-plugin/)) to identify outliers in log patterns. Such ML-based detectors could, for example, learn normal login times for each user and alert on deviations.

Findings and Alerts.  
When a detector’s rule condition is met by incoming log data, the system generates a security finding to highlight that event. Not every finding is a confirmed incident, but each represents an event worth investigating. Security analysts can search and filter these findings by severity or log type to prioritize their analysis.

OpenSearch gives users the ability to define alerting conditions. When such conditions are met, OpenSearch sends an alert to the designated channel (email, Slack, PagerDuty etc.). Alerts can be tailored to trigger on single-rule matches or only when multiple rules are detected.

Correlation of Events.

A powerful feature of OpenSearch Security Analytics is its ability to correlate multiple signals across different log sources. The built-in correlation engine can link findings from different types of logs to identify complex attack patterns spanning multiple systems.[1](https://opensearch.org/docs/latest/security-analytics/#:~:text=Security%20Analytics%20is%20a%20security,responding%20effectively%20to%20potential%20threats)

For example, a sequence of events like a VPN login from a new location, followed by a privileged action in a server log, and an abnormal outbound network connection could be correlated into one incident.

The correlation engine uses defined rules (“correlation rules”) to specify these multi-step threat scenarios and can display a visualization (a “correlation graph”) of how disparate events relate to each other.

This cross-log correlation increases confidence that an alert represents a real incident by combining clues from various sources. Such capabilities, typically found in advanced SIEMs, help analysts see the bigger picture of an attack and reduce false positives.

## Log Analysis with OpenSearch

### OpenSearch is well-suited for log analysis because it can ingest and index massive amounts of data from numerous sources, and then query that data quickly.

### Security teams benefit from being able to query recent and historical logs in one place. For example, an analyst can query web server logs, DNS logs, and authentication logs simultaneously to investigate an incident, something that would be cumbersome if those logs resided in separate silos.

### Data Normalization. Data normalization is important for building generalizable detection rules and dashboards that work across different log sources. When aggregating logs from many sources, a common challenge is that each source has its own format (different field names and structures). OpenSearch’s Security Analytics plugin includes field mappings for common log types.[1](https://opensearch.org/docs/latest/security-analytics/#:~:text=Security%20Analytics%20is%20a%20security,responding%20effectively%20to%20potential%20threats) Additionally, OpenSearch allows users to define mappings and ingest pipelines to normalize data.

### Data Visualization. Once logs are indexed and normalized, analysts can create visualizations with OpenSearch Dashboards to enhance situational awareness. For example, users can build charts showing trends of failed logins over time or a geographic map of login locations.

### Search. OpenSearch Dashboards supports interactive querying. A security analyst can filter the view to a specific timeframe or drill down on a particular host or user to see all related events.

### OpenSearch’s search capabilities also enable ad-hoc log analysis and threat hunting. Analysts can run queries to hunt for subtle signs of compromise that might not trigger an alert, such as searching across all logs for a particular filename associated with malware.

### Event Correlation. OpenSearch can also perform cross-source event correlation. Even outside of the automated correlation engine for alerts, an analyst can manually cross-correlate by querying for related identifiers. For instance, after spotting an unusual login in authentication logs, the analyst might search the VPN logs and DNS logs for the same user or IP around that time. This process is facilitated by the SIEM having all logs indexed in one system.

### OpenSearch’s ability to search multiple indices and correlate events from different data sources helps analysts identify the root cause of an incident. If a security incident involved data exfiltration, an analyst could correlate VPN access logs, server file access logs, and external network traffic logs to see exactly what was accessed and where it was sent.

## Compliance Monitoring with OpenSearch

### Beyond threat detection, a SIEM is also valuable for compliance monitoring and auditing. Many regulations and standards (such as PCI-DSS, HIPAA, GDPR, ISO 27001) mandate that organizations log certain security-related events and keep audit trails of system activity. OpenSearch helps organizations meet these requirements by centrally collecting and retaining required logs, and by providing tools to review and report on those logs for compliance purposes.

### Centralized Audit Trails. Using OpenSearch, an organization can aggregate all of its audit logs into one place. Auditors or security teams can easily query the data to answer questions like *“Who accessed sensitive finance records in the last 6 months?”* or *“Have there been any changes to firewall rules, and were they authorized?”*.

### Real-Time Compliance Alerting. Compliance monitoring isn’t just about historical audits. It also requires continuous monitoring to ensure violations or suspicious activities are caught early. OpenSearch detectors and rules can be written not only for security threats but also for compliance policies. For instance, a user could create a rule to alert if any database containing customer data is accessed outside of business hours.

### Audit Logging and Access Control. OpenSearch includes features to ensure the integrity and security of the log data. It provides audit logging capabilities that track access to the OpenSearch cluster and any changes made. This logging is useful for demonstrating that the SIEM data is protected.[4](https://opensearch.org/docs/latest/security/audit-logs/index/#:~:text=Audit%20logs%20let%20you%20track,where%20to%20store%20the%20logs)

### OpenSearch can log events like user login to the SIEM, attempts to query or delete data, and changes to roles/permissions. These audit logs help answer “who watched the watchers” – ensuring that all access to sensitive logs is recorded. In a compliance context, this means users can show that only authorized individuals accessed the audit data and that every access is traceable.

### Reporting and Retention. Compliance audits often require generating reports. With OpenSearch Dashboards, teams can create saved queries and visualization panels that serve as compliance reports. These can be exported or shown to auditors to satisfy evidence requirements.

–

### In summary, OpenSearch can serve as a the backbone to a comprehensive SIEM solution. Its ability to index, normalize, store, and make searchable logs from disparate sources makes it a powerful tool. Using Sigma Rules and ML-commons, users can identify and alert on security threats. Additionally, the visualization tools included in OpenSearch Dashboards increase situational awareness and make compliance reporting easier.

Keep in mind that OpenSearch is not as plug-and-play as other SIEM options. Reach out to trusted providers, such as my company Dattell, for information on implementing and managing an OpenSearch SIEM solution. Learn more about [Dattell’s OpenSearch SIEM Support Service](https://dattell.com/data-architecture-blog/opensearch-siem-support-service/).