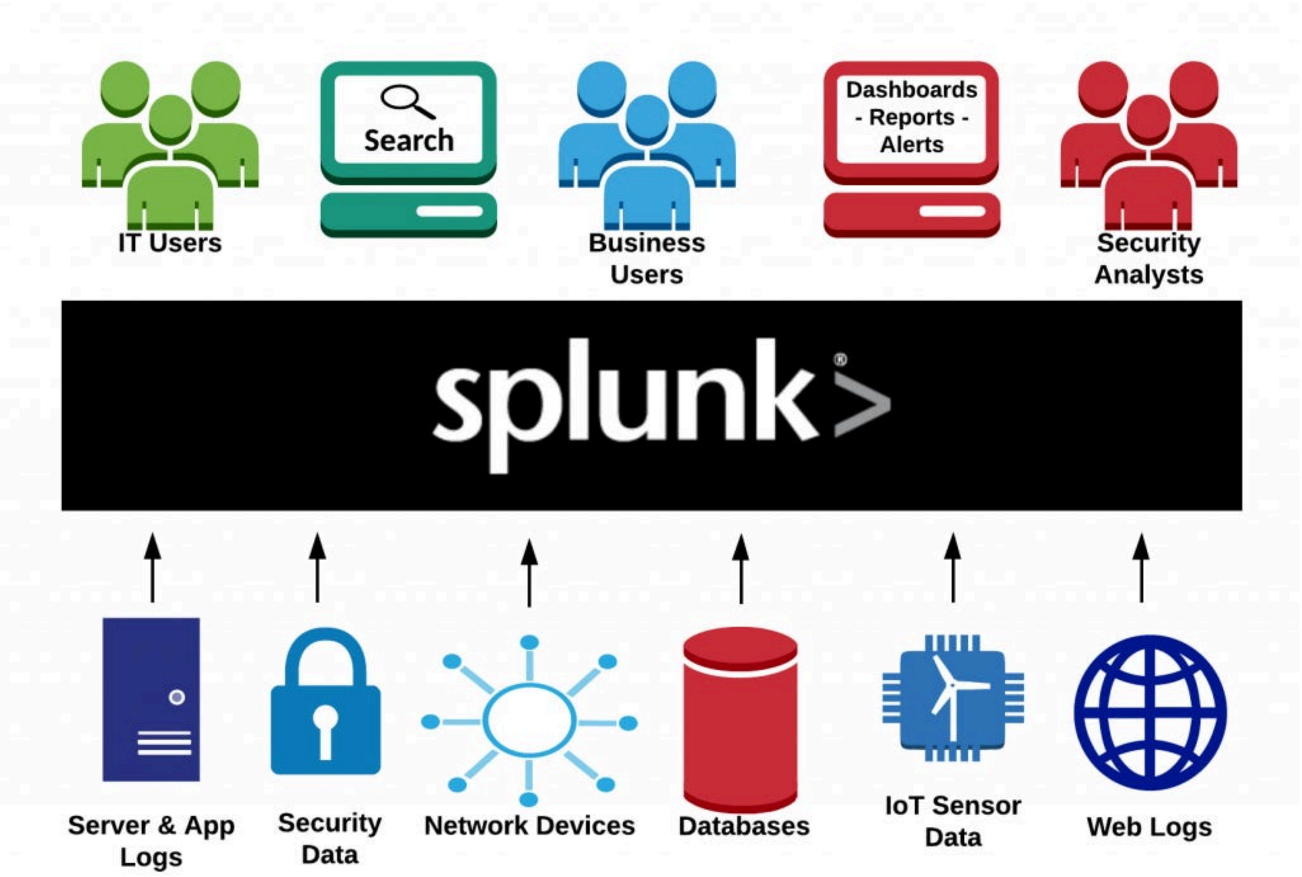
Top 10 Search Queries for Splunk



InfoSecLabs

This document provides an overview of the top 10 search queries commonly used in Splunk, a powerful platform for searching, monitoring, and analyzing machine-generated big data via a web-style interface. These queries are essential for users looking to extract meaningful insights from their data, troubleshoot issues, and enhance operational intelligence.

1. Basic Search Query

index=* | stats count by sourcetype

This query retrieves the count of events for each sourcetype across all indexes, providing a high-level overview of data distribution.

2. Search by Time Range

index=web_logs earliest=-24h | stats count

This query searches the `web_logs` index for events from the last 24 hours, allowing users to analyze recent activity.

3. Filtering by Host

index=security_logs host=server1 | stats count

This query filters events from the `security_logs` index specifically for `server1`, helping to focus on a particular host's security events.

4. Error Rate Analysis

index=application_logs "error" | timechart count by host

This query searches for occurrences of "error" in the `application_logs` index and visualizes the count over time for each host.

5. User Activity Monitoring

```
index=access_logs user="john.doe" | stats count by action
```

This query tracks the actions performed by a specific user, `john.doe`, in the `access_logs` index, providing insights into user behavior.

6. Top IP Addresses

```
index=network_logs | top src_ip
```

This query identifies the top source IP addresses in the `network_logs` index, which can help in understanding traffic patterns or potential threats.

7. Anomaly Detection

```
index=system_logs | timechart avg(cpu_usage) by host
```

This query calculates the average CPU usage over time for each host in the `system_logs` index, useful for detecting anomalies in resource usage.

8. Event Correlation

```
index=security_logs OR index=application_logs | stats count by event_type
```

This query correlates events from both `security_logs` and `application_logs`, providing a comprehensive view of different event types.

9. Geolocation Analysis

```
index=geo_logs | iplocation src_ip | stats count by Country
```

This query enriches the `geo_logs` data with geolocation information based on source IP addresses and counts events by country.

10. Alerting on Thresholds

```
index=performance_logs | stats avg(response_time) as avg_response_time | where avg_response_time > 500
```

This query calculates the average response time from `performance_logs` and filters results to show only those exceeding 500 milliseconds, useful for setting up alerts.

By utilizing these top search queries, Splunk users can effectively navigate their data, derive insights, and enhance their operational capabilities.