



# Welcome

## Introduction To SOC/SIEM



# What is SOC/SIEM?

- SOC(Security Operations Center) is a centralized team that monitors, detects, and responds to cybersecurity threats in an organization.
- SIEM(Security Information and Event Management) is a tool that collects, analyzes, and correlates security logs to detect and respond to threats.



# Introduction: The ELK Stack

- The **ELK Stack** (Elasticsearch, Logstash, and Kibana) is a powerful open-source log management and analytics solution used for real-time data monitoring and visualization.
- **Elasticsearch** is a distributed search and analytics engine that indexes and retrieves log data efficiently, while **Logstash** processes and ingests logs from various sources, transforming and forwarding them to Elasticsearch.
- **Kibana** provides a user-friendly interface for visualizing data through dashboards and graphs, making it easier to analyze security events, system performance, and application logs. Often used in **SIEM** solutions and Security Operations Centers (SOC), ELK enables organizations to detect anomalies, track incidents, and improve operational efficiency by centralizing log data analysis.



# Introduction: Metadata

- Metadata is data that describes other data, providing context such as timestamps, source IPs, file types, or user activity. Different ingestors (such as Logstash, Fluentd, or Splunk) may generate different metadata for the same information because they process and enrich logs uniquely.
- For example, if a firewall log is ingested by both Logstash and Splunk, Logstash might tag it with fields like **logsource:firewall1** and **@timestamp**, while Splunk could label it as **host=firewall1** and **index\_time**, leading to variations in how the same log is stored and interpreted.
- These differences can impact SIEM correlation, searchability, and analysis, requiring normalization to ensure consistency across platforms.



# Tips

Analytics > Discover should be one of your first steps!

A screenshot of the Elastic Stack interface. At the top left is the elastic logo. To its right is a search bar with the placeholder "Find apps, content, and more." Below the search bar are three navigation items: a menu icon, a "D" icon, and a "Home" button. The main area has a dark background with two cards. The first card, on the left, is yellow and contains the Elasticsearch logo (a stylized "E" icon) and the text "Elasticsearch". Below it, a subtitle reads: "Create search experiences with a refined set of APIs and tools." The second card, on the right, is blue and contains the Analytics logo (a stylized "K" icon). It is highlighted with a red border. Below it, a subtitle reads: "Explore, visualize, and analyze your data using a powerful suite of analytical tools and applications." Both cards have a black footer bar.

# Tips



Analytics > Discover should be one of your first steps!

A screenshot of the Elastic Analytics interface. At the top, there's a navigation bar with the elastic logo, a search bar, and a dropdown menu. Below the navigation is a title "Analytics" with a "Discover" tab selected. The interface is divided into two main sections: "Dashboard" on the left and "Discover" on the right. The "Discover" section is highlighted with a red border. Both sections contain various data visualizations like line charts, bar charts, and pie charts.



# Tips

The Data View determines what type of logs will be displayed for you!

A screenshot of a log search interface, likely from Elasticsearch or Logstash. The top navigation bar shows "Data view" and "logs-\*". Below this is a search bar with placeholder text "Filter your data using KQL syntax". A red box highlights the "Data views" section. This section includes a search bar for "Find a data view", a "Create a data view" button, and a list of available data views: "apm-\*-transaction\*", "auditbeat-\*", "endg...", "winlogbeat-\*", "\*elastic-cloud-logs-\*", "logs-\*" (which is checked), and "metrics-\*". A message below states "No available fields containing data.". To the right, a large error message says "No results match your search criteria". It suggests trying to extend the time range, and lists "Empty fields" (288) and "Meta fields" (4). At the bottom right is a blue button labeled "Search entire time range".

No results match your search criteria

Here are some things to try:

- Extend the time range

Search entire time range



# Tips

Timestamp is important!

The screenshot shows the Elasticsearch Discover interface. At the top, there's a search bar with placeholder text "Find apps, content, and more." and a "Discover" tab selected. Below the search bar is a toolbar with "Data view" and "logs-\*" buttons, a filter icon, a plus icon, and a search input field with placeholder "Filter your data using KQL syntax". To the right of the toolbar are buttons for "Try ES|QL", "Inspect", and file operations ("+", "Save", "Open"). A red box highlights the time range selector, which is set to "Last 15 minutes".

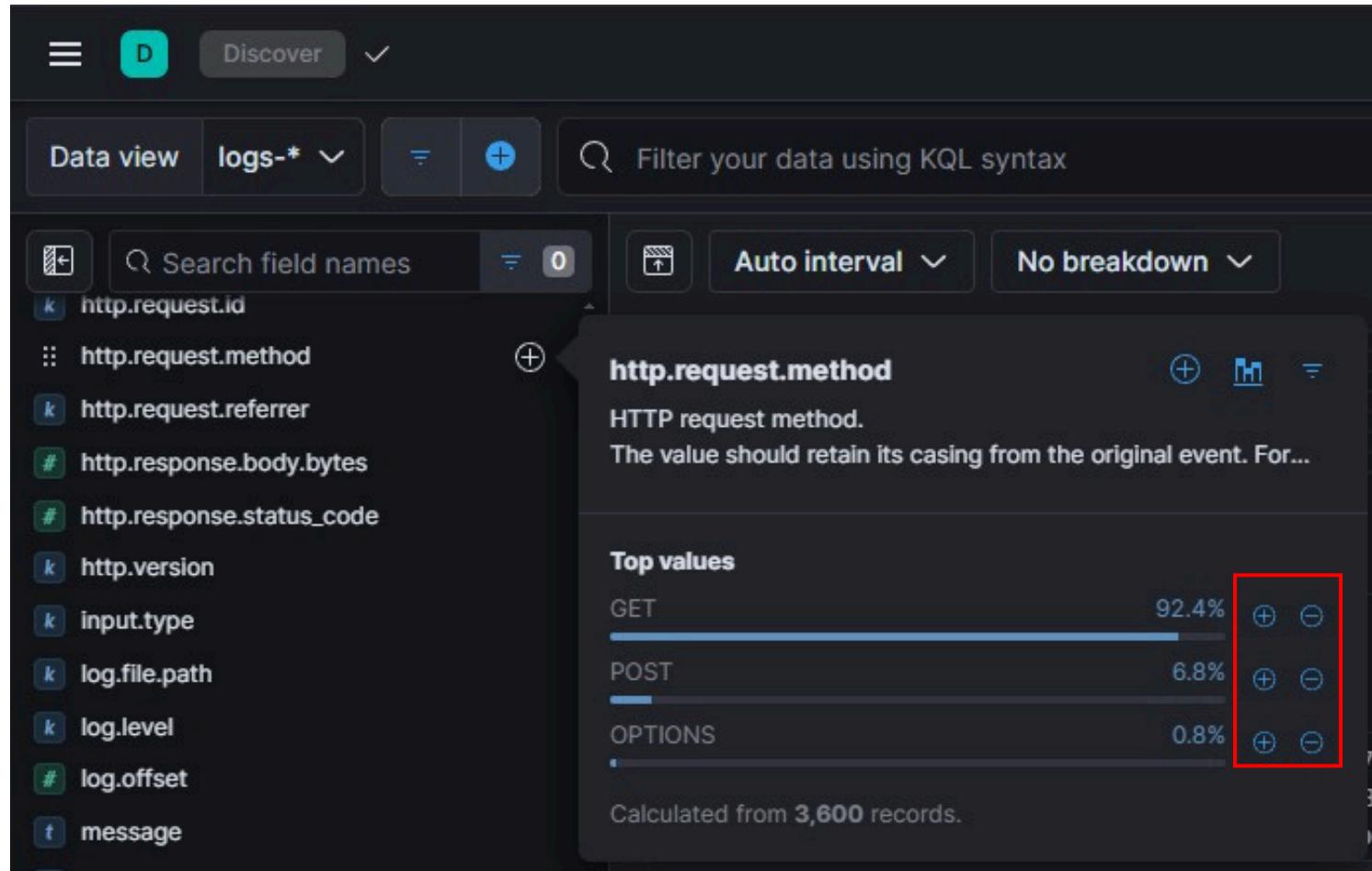
On the left, there's a sidebar titled "Search field names" with a dropdown arrow. It lists "Popular fields" (1 item: "process.working\_directory") and "Available fields" (0 items). Below this, it says "No available fields containing data." and provides a "Try:" section with a bullet point: "Extending the time range".

The main content area displays a message: "No results match your search criteria". Underneath, it says "Here are some things to try:" followed by a bullet point: "Expand the time range". At the bottom of this area is a blue button labeled "Search entire time range". To the right of the message is a decorative graphic of a magnifying glass with a dashed trail and a pink exclamation mark.



# Tips

Filters are very important!





Here are the domain and credentials for the Threat Hunting challenges.

Have fun! 😊

**Domain:** <https://cyberblitz.ddns.net/>

**Username:** cyberblitz2025

**Password:** cyberblitz2025!

**Sample Flag Format:** CyberBlitz2025{flag}

**CyberBlitz2025{IHAVEREADTHISELKDOCUMENTATION}**