



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 thatcollects, 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.



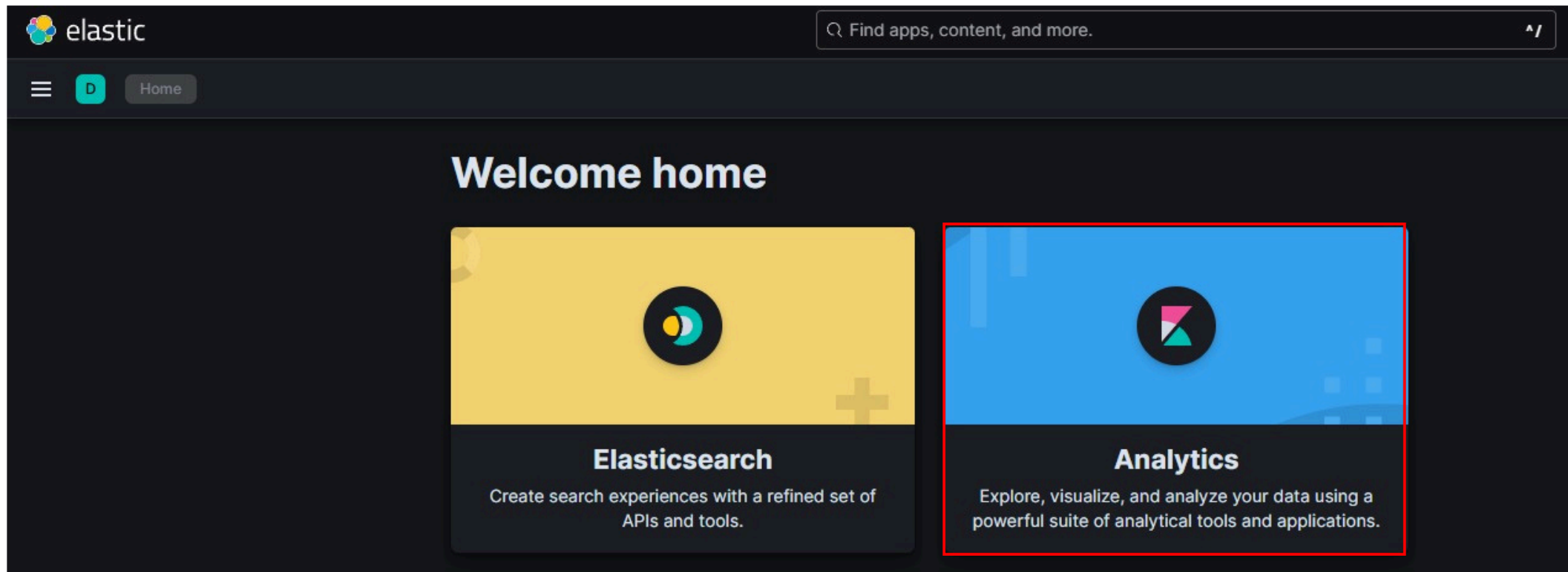
Introduction: Metadata

- 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



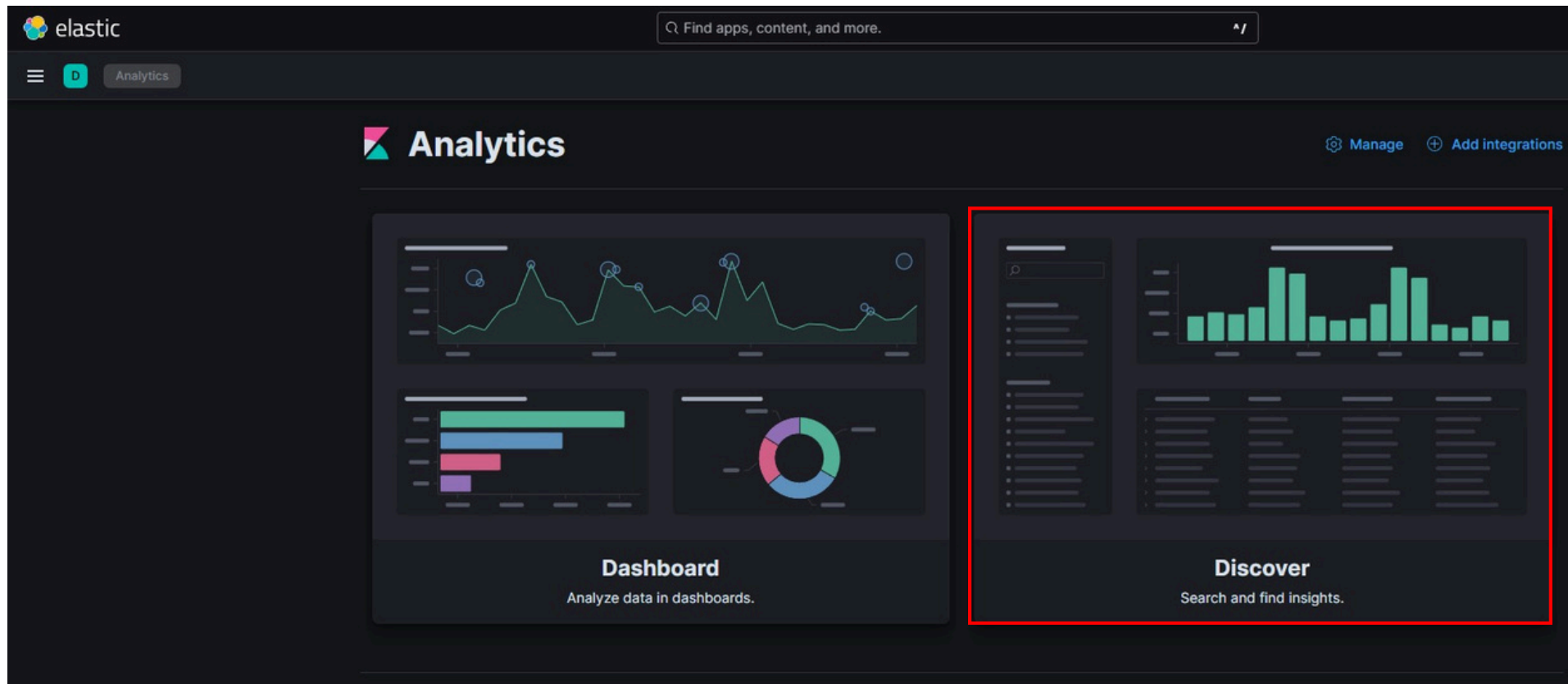
Analytics > Discover should be one of your first steps!



Tips



Analytics > Discover should be one of your first steps!



Tips



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

The screenshot shows the Elastic Search interface. At the top, there is a "Data view" dropdown menu with "logs-*" selected. Below this, a search bar for "Data views" is visible, with a list of suggestions: "apm-*transaction*,auditbeat-*,endg...,winlogbeat-*,-*elastic-cloud-logs-*", "logs-*" (which is checked), and "metrics-*". Below the search bar, there is a section titled "Try:" with a list of suggestions: "Extending the time range". To the right of this list, there are two buttons: "Empty fields" with a count of "288" and "Meta fields" with a count of "4". On the right side of the interface, a large message states "No results match your search criteria" and provides a list of suggestions: "Expand the time range". At the bottom right, there is a blue button labeled "Search entire time range".

Tips



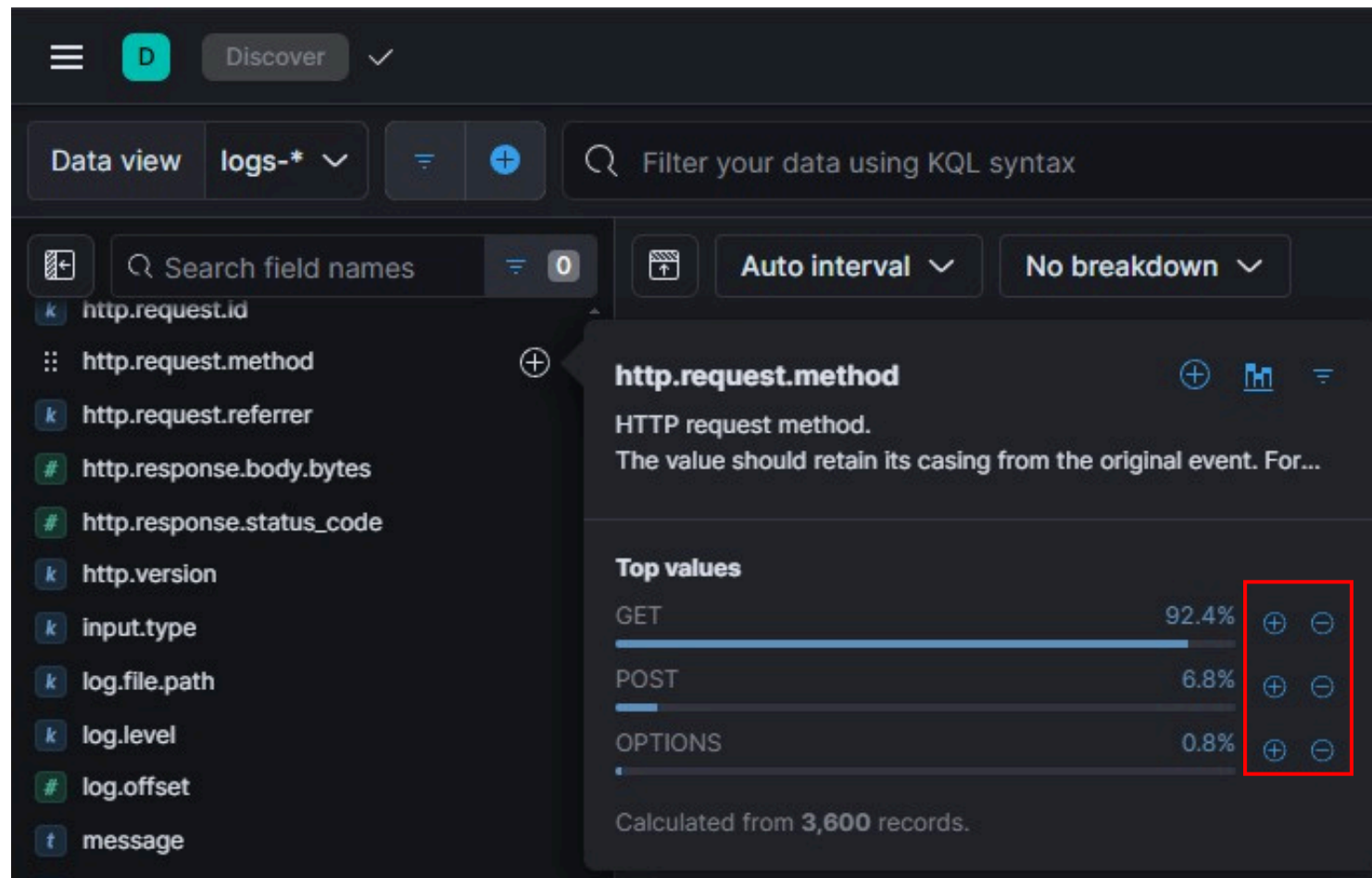
Timestamp is important!

The screenshot shows the Elastic Discover interface. The top navigation bar includes the Elastic logo, a search bar, and buttons for 'Try ES|QL', 'Inspect', and a user profile icon. Below the navigation bar, the 'Data view' section shows 'logs-*' selected. A search bar prompts the user to 'Filter your data using KQL syntax'. The left sidebar displays field filters: 'Popular fields' (1), 'Available fields' (0), 'Empty fields' (288), and 'Meta fields' (4). The main area displays 'No results match your search criteria' with a suggestion to 'Expand the time range' and a 'Search entire time range' button. A red box highlights the 'Last 15 minutes' and 'Refresh' buttons in the top right corner.

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}