Investigating with ELK 101

## **Task 1 – Introduction**

* **ELK Stack** = Elasticsearch, Logstash, Kibana (often with Beats).
* Purpose: Centralized log collection, search, and visualization for incident investigation.
* Use case: Security analysts use ELK for **log correlation**, **incident response**, and **threat hunting**.

## **Task 2 – Incident Handling Scenario**

* The lab simulates a **security incident** where you must:
  + Gather evidence from logs.
  + Identify suspicious patterns.
  + Use Kibana and KQL to query events.
  + Create visualizations for reporting.

## **Task 3 – Elastic Stack Overview**

* **Elasticsearch** – Search and analytics engine; stores and indexes logs.
* **Logstash** – Data processing pipeline; ingests, transforms, and sends logs to Elasticsearch.
* **Beats** – Lightweight data shippers (e.g., Filebeat for logs, Packetbeat for network data).
* **Kibana** – Web interface for search, visualization, and dashboards.

## **Task 4 – Kibana Overview**

* GUI to query and visualize Elasticsearch data.
* Key features:
  + **Discover** tab: Search and filter logs.
  + **Visualize**: Create charts and graphs.
  + **Dashboards**: Combine multiple visualizations.
  + **Security App** (if enabled): Security event monitoring.

## **Task 5 – Discover Tab**

* Allows you to:
  + View raw logs.
  + Filter by time range.
  + Apply search queries.
  + Save searches for later use.
* Useful for initial **log exploration** and **threat hunting**.

## **Task 6 – KQL Overview (Kibana Query Language)**

* Syntax for filtering and searching logs.
* Examples:
  + host.name : "webserver01"
  + event.action : "login" AND event.outcome : "failure"
  + Wildcards: file.name : "\*.exe"
* Supports logical operators: AND, OR, NOT.

## **Task 7 – Creating Visualizations**

* Turns data into:
  + Bar charts
  + Line graphs
  + Pie charts
  + Maps
* Helps identify trends, anomalies, and attack patterns.
* Example: Visualizing failed logins by username.

## **Task 8 – Creating Dashboards**

* Combine multiple visualizations into one view.
* Example SOC dashboard:
  + Failed logins trend
  + Top source IPs
  + File changes over time
* Useful for **continuous monitoring** and **executive reporting**.

## **Task 9 – Conclusion**

* ELK Stack is a powerful **SIEM-like** platform for log management and security investigations.
* **Workflow**:
  1. Gather logs (Beats/Logstash)
  2. Store and index (Elasticsearch)
  3. Search and analyze (Kibana)
  4. Visualize and report (Visualizations & Dashboards)
* Helps in **real-time detection** and **post-incident forensics**.

