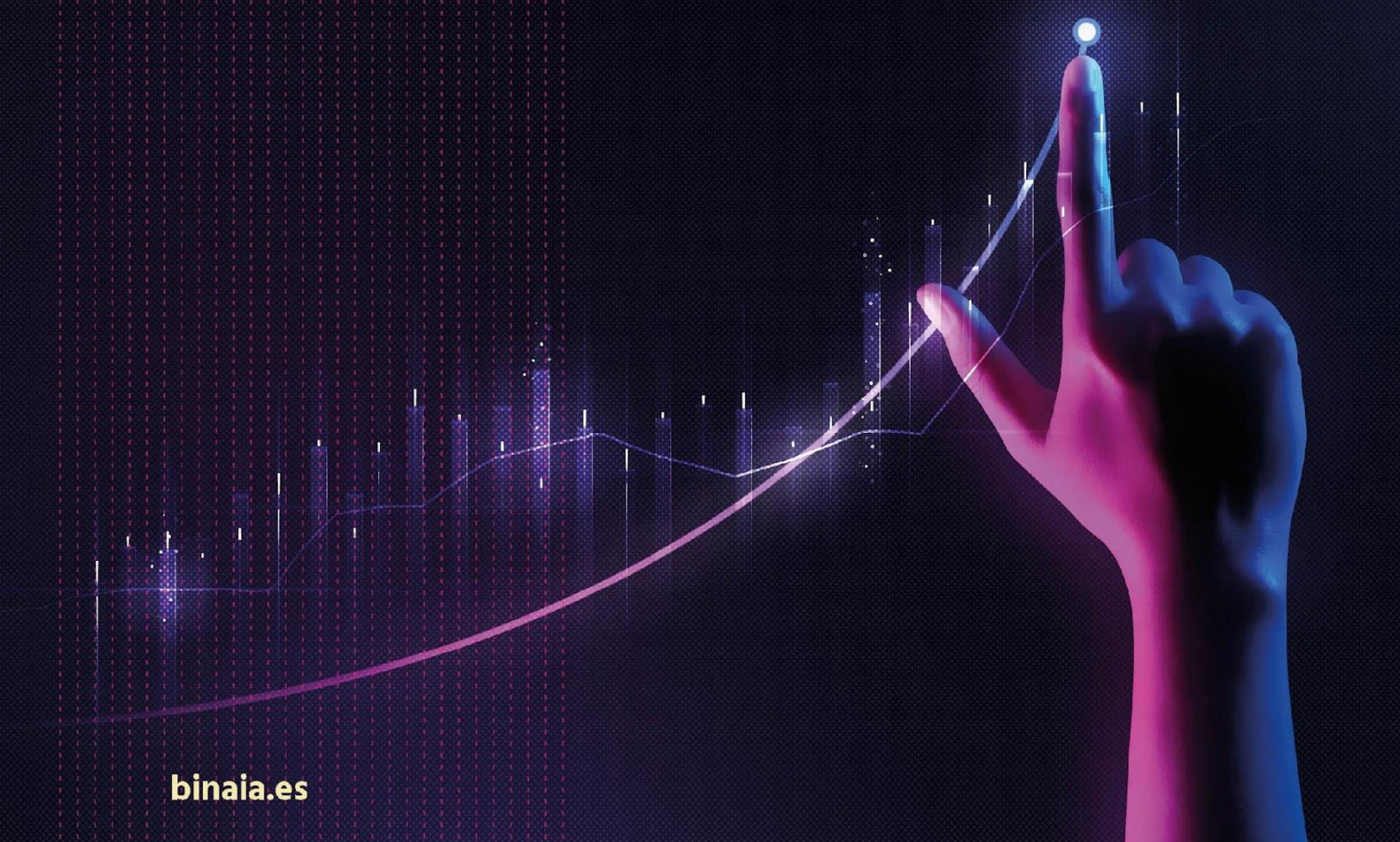
BINAIA

BCIT in

ELK Stack



binaia.es

Objetivos

El principal objetivo de la formación es preparar a los alumnos para que conozcan y dominen el Stack de ELK.

En concreto, los objetivos específicos de la formación son:

- Conocer y dominar ElasticSearch
- Conocer y dominar Logstash
- Conocer y dominar Kibana

Requisitos

Es necesario tener conocimientos previos en logs, motores de búsqueda y visualización de datos.

Metodología

En esta formación, el aprendizaje se llevará a cabo de una **forma dinámica** con una enseñanza teórica y práctica compaginando ambas mediante la realización de ejercicios que permitan hacer uso de todo lo aprendido buscando asentar el conocimiento.

Programa

El programa se estructura en los bloques que se describen a continuación:

Bloque 1: Metricbeat

- Configuración: Input/Output
- Output – stdout() - consola
- Logstash
- Elastic
- Dashboards Kibana

Bloque 2: Logstash

- Configuración: Input/Output
    - Input: Metricbeat
    - Output: stdout()
- Configuración: Input/Filter/Output
    - Filter: Modificación de campos (Mutate, rename, date...)
- Configuración: Input/Filter/Output
    - Output: Elasticsearch
- Sacar estadísticas por output
- Sacar por consola con codec:json
- Rubydebug
- Condicionales
- Dates
- Diferentes inputs, stdin, api, beat
    - Condicionales
    - Aggregate para añadir tag y que sirva para el filtrado, y decidir a dónde mandar
- Diferentes stdout, elastic

- Cómo actúa logstash con diferentes entradas sin un filtro y ver errores
- Piplines.yml
- Diferentes fuentes de info a través de logstash sin errores

Bloque 3: ElasticSearch

- Consultas básicas
    - CURL
    - API Kibana
- Creación/acciones de un índice
    - A mano desde la interfaz
    - Desde API Kibana
- Configuración índice
    - Políticas de vida
    - Templates
- RollUp
    - Aliases
- Tokenizadores posibles
- Índice invertido
- Transformaciones en índices

Bloque 4: Kibana

- Tipos de gráficos
- Dashboards
- Series temporales
- Mapas

binaia.es