BLueTeam.id

Cert No : BTDAT-401/2022/02

CERTIFICATE

Of Completion

This Acknowledge That

Muhammad Amzar Fadliatma Putra

Attended and performed hands-on to complete in :

Data Analytics Tools II

30th of May - 2nd of June 2022

Sida Nala Rukma Januarto

Instructor

DATA ANALYTICS TOOLS II

Day 1

- Logging and Log management
- Elastic Stack Overview
- Getting Started with Elasticsearch
- Installing Elasticsearch & Kibana
- Understanding API
- CRUD operations
- Querying Data
- Mappings
- Node Types

Hands on Labs Day 1:

- Logging with Syslog Server
- Installing Elasticsearch & Kibana
- Elasticsearch API
  Create / Insert document
  Read document
  Update Document
  Delete Document
  Insert Document Bulk
  Mapping Document

Day 2

- Understanding Shards
- Troubleshooting Elasticsearch
- Pagination
- Sorting
- Filter
- Fuzziness
- Partial Matching
- Importing Data
- Logstash Overview
- Installing Logstash
- Logstash Integration
- Logstash Configuration
- Logstash Plugins

Hands on Labs Day 2:

- Elasticsearch API
  Pagination
  Sorting
  Filter
  Fuzziness
  Partial Matching
- Installing Logstash & Beats
- Logstash integration with:
  TCP/UDP Raw Data
  Syslog Server
  Beats
  JDBC Mysql Database
  HTTP API
- Centralized logging using Elastic Stack

Day 3

- GROK
- Logs Parsing
- Logstash Filter
- Data Enrichment
- Using Beats
- Aggregating Data
- Time Series
- Using Kibana
- Playing with Kibana
- Kibana configuration
- Analysing logs with Kibana

Hands on Labs Day 3:

- Setup Dashboard
- Config Beats
- Logstash Filter
- Visualization and Analysis Log using Elastic Stack
  Access log
  Syslog/Auth log
- Create Dashboard

Day 4

- Kibana Dashboard
- Importing Data using Data Visualizer
- Reindex
- Heap Sizing
- Stack Management
- Snapshot
- Clustering
- Availability
- Scaling Elastic Stack Node
- Securing Elastic Stack
- Working Elasticsearch with Jupyter notebook

Hands on Labs Day 4:

- Working with maps Visualization
- Elasticsearch API:
  Aggregation
  Reindex
  Snapshot
- Setup Clustering (tbd)
- Monitoring Elastic Stack
- Securing Elastic Stack
- Working Elasticsearch with Jupyter Notebook

BLueTeam.Id