Ingesting Data into Elasticsearch

Aaron Rosenmund
AUTHOR EVANGELIST – SECURITY OPERATIONS

@arosenmund www.AaronRosenmund.com

Implementation Scenario

Globomantics security analyst

Supporting continuous monitoring and detections

You think “I could use the elastic stack for this” and you are correct

Overview

Interacting with elasticsearch in Kibana

Creating and index

Manual data ingestion

Automated data ingestion

Working with index patters

Elastic Stack

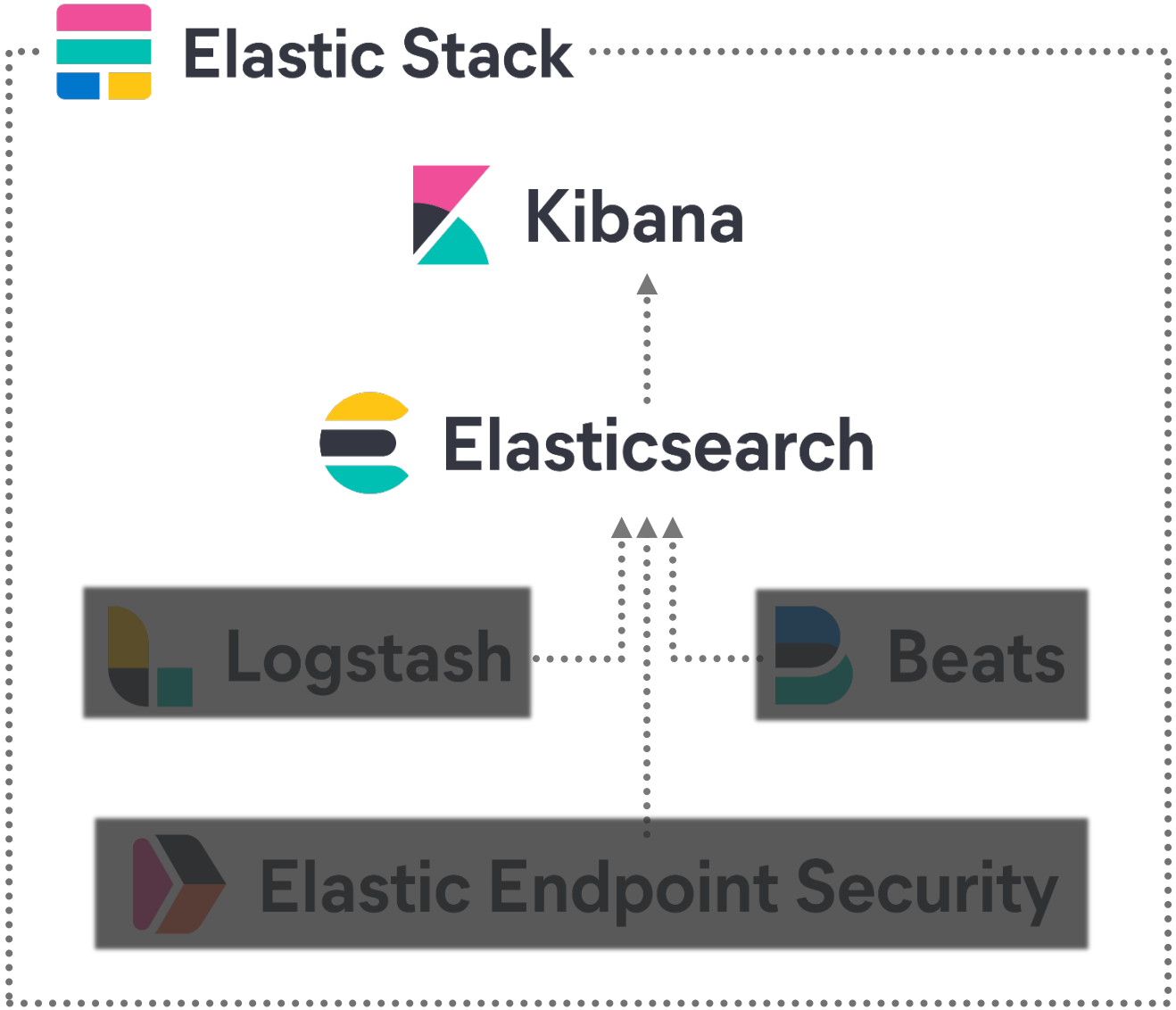
Elasticsearch

Kibana

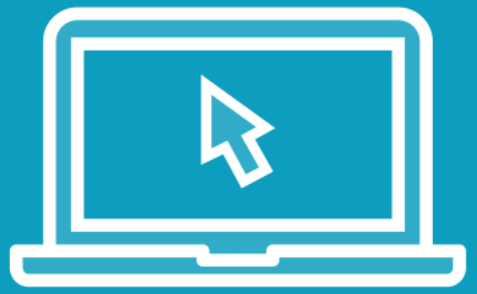
Logstash

Beats

Endpoint Security



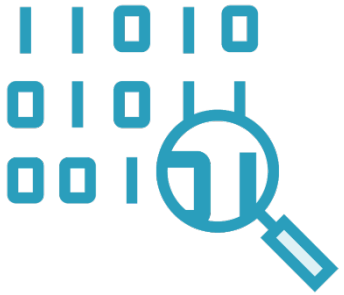
Demo



Connecting Kibana to Elasticsearch

Configuration, stack monitoring with Kibana connection

Components of Kibana

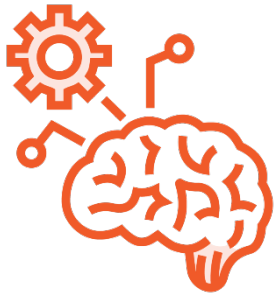


Discover

Dashboard

Canvas

Maps



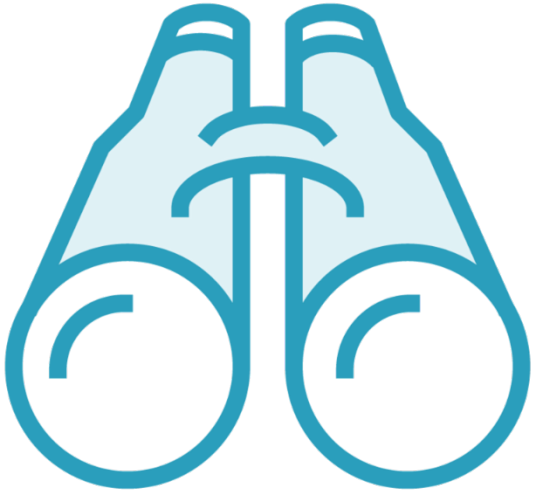
Machine Learning

Visualize

Demo

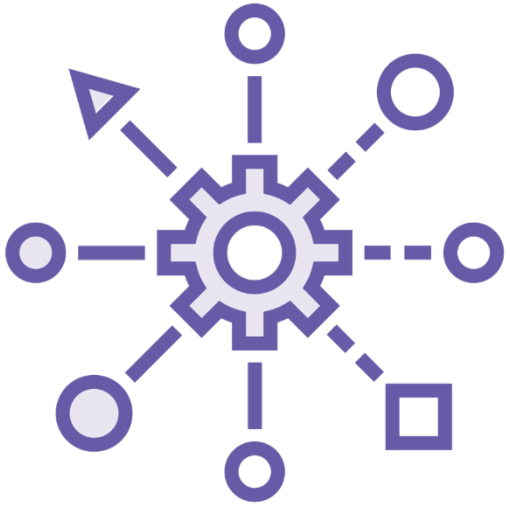
Demo the components of Kibana

Additional Kibana Interfaces



Observability

Security



Management

Index

In elastic search, an index is a bucket, customized to hold the data from a specific source.

```
# Create an index named “securityinfo”

# dev tools provides a platform for you to interact directly with the REST API

PUT /securityinfo
```

Manual Elasticsearch Interaction

Rest API is leveraged for basic and advanced functions

You can access the API directly through dev tools in Kibana

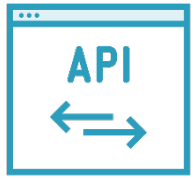
This is not the only way to interact with Elasticsearch; don’t get scared away

Demo

Demo Index Creation

Where Is the Data?

How to Get Data into an Index



Rest API

Upload through Kibana

Beats & Logstash

```
curl -XPOST http://elastic-node/<indexname>/_doc/

-H 'Content-Type: application/json'

-d'

{

  "@timestamp": "2021-01-05T10:10:10",

  "message": "Protocol Port Mis-Match",

  "dst": {

    "ip": "192.168.1.56",

    "port": "88",

  }

}

'
```

- Using curl to push a POST request to the desired index
- _create or _doc
- Content type must be set to "application/json"
- Document information in JSON

Demo

Demo manual curl push

Drag and drop azure activity

Elastic Beats

Light weight data shippers, that will package up streamed or static data, normalize and parse it to the ECS standard and push it into the elastic stack.

Filebeat

Metricbeat

Packetbeat

Winlogbeat

Auditbeat

Heartbeat

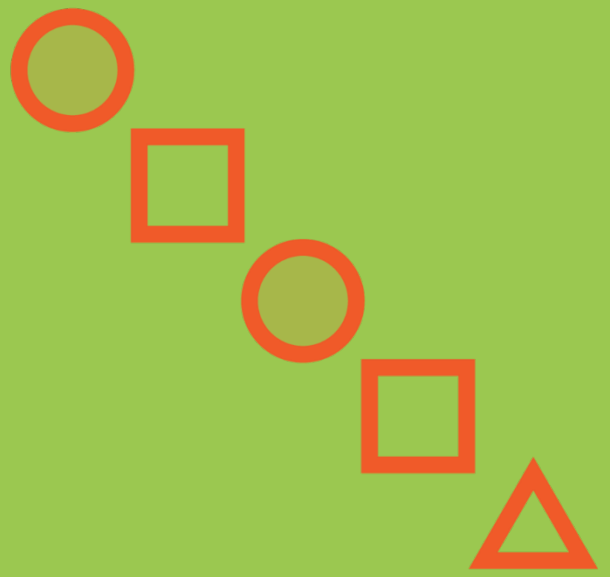
Functionbeat

Elastic Agent

Anti-malware agent that operating in the same way as any other EDR

Demo

Filebeats demo



Index pattern

Selects the indices to be aggregated by matching a string pattern to the name of individual index. All matching indices are grouped together and explorable under this pattern.

Demo

Demo index pattern use.

Summary

- Index patterns
- Beats
- Rest API index creation
- Rest API elastic interaction
- Kibana configuration