Blueliv.

ELK stack Documentation

AUTHOR: Blueliv

DATE: September 20, 2016

Contents

Introduction

1.1 The ELK stack

The ELK stack contains **E**lasticsearch, **L**ogstash, and **K**ibana. Although they have all been built to work exceptionally well together, each one is a separate open source project that is driven by Elasticsearch. The role of each of these technologies is divided as follows:

Logstash Tool for managing events and logs. You can use it to collect logs, parse them, and store them for later use, such as searching. You can collect several different types of data from different sources (logs, HTTP, TCP, Kafka, etc) and then filter or transform them.

Elasticsearch Search server based on Lucene. It provides a distributed, full-text search engine with a RESTful web interface and schema-free JSON documents. You can use it to index and aggregate data from Logstash.

Kibana Browser based analytics and search dashboard for Elasticsearch. You can set-up dashboards with graphics and tables to visualize your indexed and aggregated data from Elasticsearch.

1.2 Logstash Plugins

Since version 1.5, there is a new plugin management system for Logstash. Plugin repositories are now located at Github. Plugins are now self-contained Ruby gems hosted in RubyGems. Logstash comes with a script called `plugin`, which is used to install the extra plugins. All plugins can be found listed and searchable at Github. There are three kinds of Logstash plugin:

Input To provide input data into Logstash.

Filter To filter data from a given input.

Output To save the filtered data anywhere you want, such as Elasticsearch, for indexing and searching data.

1.3   Blueliv on ELK

Blueliv automatically integrates Blueliv's Cyber Threat Intelligence into ELK stack, providing an *input* plugin for Logstash. The use of this app will add Cyber Threat Intelligence to your existing data, addressing a comprehensive range of cyber threats including compromised URLs, domains, IPs, etc. to turn global threat data into predictive, actionable intelligence specifically for your enterprise and the unique threats it faces.

Our powerful networks of specialized search engines constantly scour the web for up-to-the- minute data and delivers real-time actionable information.

Unsurpassed cyber threat intelligence, now at your disposal.

Installation

2.1 Requirements

This plugin was developed and tested against Logstash 1.5.0, so it supports this and newer versions. Older versions are **not** supported due to changes in Logstash plugin API. As of Elasticsearch and Kibana, you must use Elasticsearch version $\geq$ 2.4.0 and Kibana $\geq$ 4.6.0 in order to work with Elasticsearch 2.4.x.

2.2 Blueliv Plugin

Blueliv provides an *input* plugin, delivering data about active Crime Servers and Bot IPs. To install it, please run the following command in the directory where you installed Logstash:

```
> bin/plugin install -version 1.0.1 logstash-input-blueliv
```

2.3 Configuration

Before using our plugin, you should configure your API Key (get yours here) and the feeds that you want to receive. The plugin has the following configuration parameters:

api_url the URL of the API. By default its value is `https://api.blueliv.com`, but you should change it if you are using our Free API (`https://freeapi.blueliv.com`).

api_key API key to access our feeds. This parameter is **mandatory** in order to get the plugin working. You can get your Free API key here or contact us via email in order to get a commercial account.

http_timeout HTTP timeout for each API call. Default: `500` seconds.

feeds it is a Ruby hash that specifies the parameters to access each one of our feeds. Each feed may be configured with the following properties:

active if the feed is active or not. Default: `false`.

feed_type the type of the feed that you want. For **Crime Servers** apart from `test` (for debug purposes) you only have all. As of **Bot IPs** you may choose between `non_pos` (all BotIPs **but** the ones from Point-of-Sale), `pos` (only from POS) or full (all of them) feed.

interval interval of polling data from our API. Default is `600` seconds (10 minutes) for BotIPs and `900` (15 minutes) for CrimeServers.

The default configuration for `feeds` parameter is available at listing 2.1.

```
{
  "crimeservers" => {
      "active" => false,
      "feed_type" => "test",
      "interval" => 900,
    }
    "botips" => {
      "active" => false,
      "feed_type" => "test",
      "interval" => 600,
    }
}
```

Listing 2.1: Default `feeds` configuration

2.3.1 Example

An example of an input configuration is shown in listing 2.2.

```
input {
  blueliv {
    api_key => "<YOUR API KEY>"
    feeds => {
      "botips" => {
        "active" => true
        "feed_type" => "non_pos"
      }
      "crimeservers" => {
        "active" => true
        "feed_type" => "recent"
```

```
            }
        }
    }
}
```

Listing 2.2: Plugin configuration example

Be aware that if you do not specify a given field, the default value will be configured. In this case, we did not touch the `interval` field for the feeds, so the defaults will apply.

Getting Started

In this chapter we are going to explain how to set-up properly a full ELK stack in order to take advantage of the cyber-threat intelligence provided by Blueliv. Please be aware that his is a configuration suggestion and you may change it to fit your needs. You may skip some of the steps if you already have configured your ELK stack.

3.1 Logstash Configuration

Our Logstash configuration is divided in two main components, as shown in listing 3.1.

input where you must set-up your API key and cyber-threat feeds that you want

output where we set-up the way we want to set-up the *output.* Our configurations go as following:

    index where we are indexing each feed in a different Elasticsearch *index,* i.e., `blueliv-crimeservers` and `blueliv-ips`.

    manage_template where we tell Logstash that we will not manage Elasticsearch *template* for our *indexes.* We explain more on this in 3.2.

    document_id we provide a `document_id` for Elasticsearch *indexes,* so when a object - such as a Crime Server - is updated, it will update its entry.

```
input {
  blueliv {
    api_key => "<YOUR API KEY>"
    feeds => {
      "botips" => {
        "active" => true
        "feed_type" => "non_pos"
      }
      "crimeservers" => {
```

```
            "active" => true
            "feed_type" => "recent"
        }
      }
    }
}
output {
  elasticsearch {
    index => "blueliv-%{@collection}"
    manage_template => false
    document_id => "%{document_id}"
  }
}
```

<center>Listing 3.1: Full Logstash configuration example</center>

You can find these configurations at our GitHub. If you are are using our Free API, you should use these configurations.

Please note that the first time you run this plugin in Logstash it may take some time to download and index all the items.

3.2 Elasticsearch Configuration

The only configuration that you need to perform in Elasticsearch is to upload Blueliv's index template, shown in listing 3.2. In order to upload it you should make a REST call to the following Elasticsearch end-point. You may use `curl` to do it. If you save our template (3.2) as `template.json`, you could just run the following command:

```
> curl -XPUT localhost:9200/_template/blueliv -d @template.json
```

```
{
    "template": "blueliv-*",
    "settings": {
        "index.refresh_interval": "5s"
    },
    "mappings": {
        "_default_": {
            "dynamic_templates": [
                {
                    "message_field": {
                        "mapping": {
```

```
                        "index"   "analyzed"
                        "omit_norms"   true
                        "type"   "string"
                    }
                    "match_mapping_type"   "string"
                    "match"   "message"
                }
            }
            {
                "string_fields"   {
                    "mapping"   {
                        "index"   "analyzed"
                        "omit_norms"   true
                        "type"   "string"
                        "fields"   {
                            "raw"   {
                                "ignore_above"   256
                                "index"   "not_analyzed"
                                "type"   "string"
                            }
                        }
                    }
                    "match_mapping_type"   "string"
                    "match"   "*"
                }
            }
        ]
        "_all"   {
            "omit_norms"   true
            "enabled"   true
        }
        "properties"   {
            "location"   {
                "type"   "geo_point"
            }
            "lastSeenAt"   {
                "type"   "date"
                "format"   "yyyy-MM-dd'T'HH:mm:ssZ"
            }
            "firstSeenAt"   {
                "type"   "date"
                "format"   "yyyy-MM-dd'T'HH:mm:ssZ"
            }
            "updatedAt"   {
                "type"   "date"
```

```
                    "format"    "yyyy-MM-dd'T'HH:mm:ssZ"
                }
                "@version"    {
                    "index"    "not_analyzed"
                    "type"    "string"
                }
            }
        }
    }
}
```

Listing 3.2: Full Logstash configuration example

You can find these configurations at our GitHub.

3.3   Kibana Configuration

In this section we will show you how to set-up your Elasticsearch indexes (3.4), create charts and data tables (3.5) and put it all together in a dashboard (3.6). In section 3.6.1 you can find the example dashboards that we have set-up.

3.4   Indexes

To access your Kibana installation you should browse to the corresponding address (by default: `http://localhost:5601`). Then you must set-up the indexes that you want to get data of. As shown in figure 3.1.

Figure 3.1: Configuring an index in Kibana.

As you may noticed, you can configure an index (e.g., `blueliv-ips`) or a pattern that has all the indexes you want (e.g., `blueliv-*`). You must select a Time-field, which will be the default field used to filter time-based events.

3.5   Charts

After configuring the indexes, you can now play with the indexed data, either through search or creating charts and data tables. If you click in `Visualize`, on top menu (3.2), you can choose one of the available charts or data table.
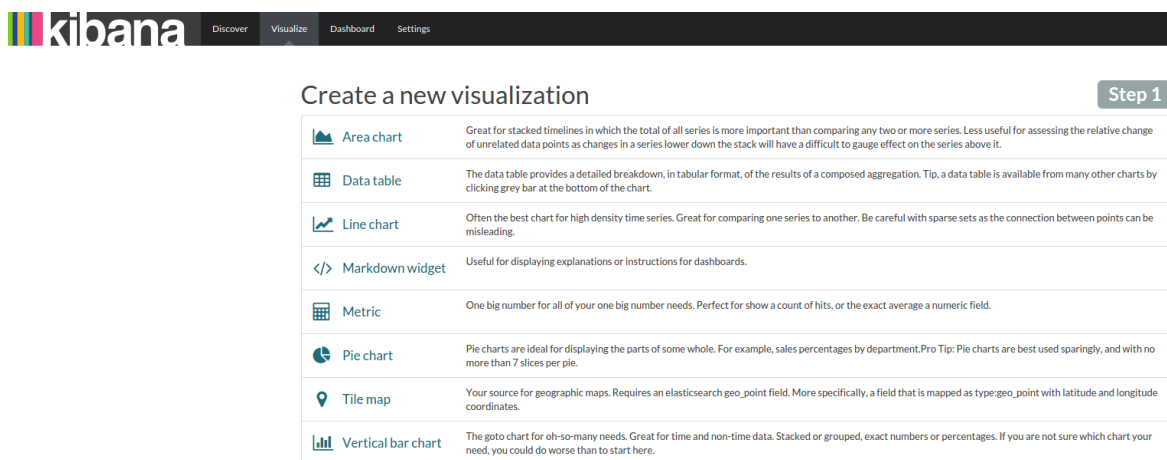

Figure 3.2: Choosing a chart in Kibana.

After that, you must choose the source for your chart or data table, either a *new search* or a saved one (3.3) on an Elasticsearch index.
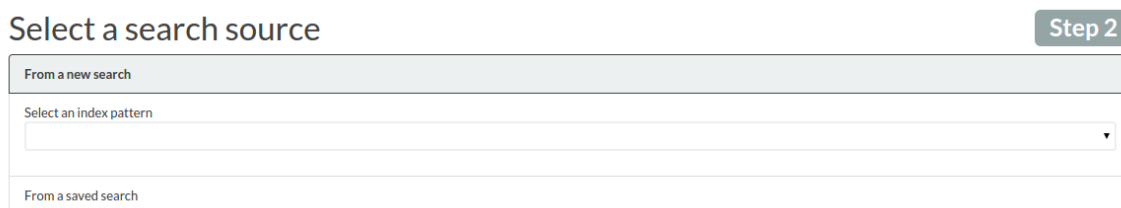

Figure 3.3: Choosing a source for a chart in Kibana.

After that you may choose the field that you want to show, as well as the aggregation (geo-location, count, average, etc). You may find some examples in section 3.6.1.

3.6 Dashboards

Kibana dashboards are just a view where you can get some of your graphs in a glance as well as rearrange them freely. If you click in `Dashboard`, on top menu (3.2), you can create a new dashboard or load an existing one. If you want to add a new graph into a dashboard, just click on `Add Visualization` button (last left-to-right in figure 3.4). After that you should choose one of the graphs (3.5) you created before (see 3.5).

Figure 3.4: Adding a new graph into a Kibana dashboard.
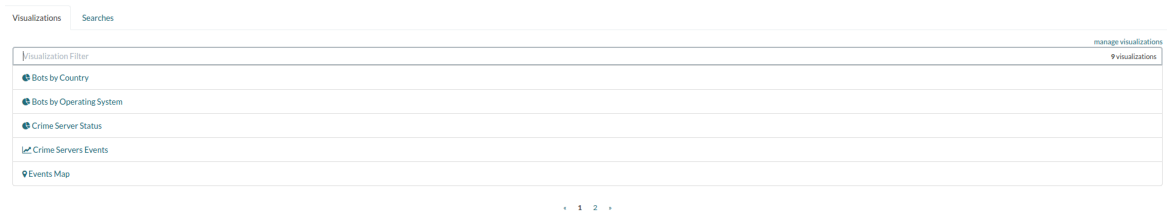

Figure 3.5: Select a saved graph to add into a Kibana dashboard.

```
[
  {
    "_id": "Bot-IPs",
    "_type": "dashboard",
    "_source": {
      "title": "Bot IPs",
      "hits": 0,
      "description": "",
      "panelsJSON": "[{\"col\":1,\"id\":\"Bot-IP-per-hour\",\"panelIndex\":1,\"
          row\":5,\"size_x\":4,\"size_y\":4,\"type\":\"visualization\"},{\"col
          \":8,\"id\":\"Top-10-Bot-IP\",\"panelIndex\":2,\"row\":1,\"size_x
          \":5,\"size_y\":4,\"type\":\"visualization\"},{\"col\":4,\"id\":\"Top
          -10-Operating-Systems\",\"panelIndex\":3,\"row\":1,\"size_x\":4,\"
          size_y\":4,\"type\":\"visualization\"},{\"id\":\"Infection-Map\",\"type
          \":\"visualization\",\"panelIndex\":4,\"size_x\":5,\"size_y\":4,\"col
          \":8,\"row\":5},{\"id\":\"Top-10-Portal-domains\",\"type\":\"
          visualization\",\"panelIndex\":5,\"size_x\":3,\"size_y\":4,\"col\":5,\"
          row\":5},{\"id\":\"Botnet-URL\",\"type\":\"visualization\",\"panelIndex
          \":6,\"size_x\":3,\"size_y\":4,\"col\":1,\"row\":1}]",
      "optionsJSON": "{\"darkTheme\":false}",
      "uiStateJSON": "{\"P-1\":{\"vis\":{\"legendOpen\":false}},\"P-2\":{\"vis
          \":{\"legendOpen\":false}}}"
```

```
    "version": 1,
    "timeRestore": true,
    "timeTo": "now/w",
    "timeFrom": "now/w",
    "kibanaSavedObjectMeta": {
      "searchSourceJSON": "{\"filter\":[{\"query\":{\"query_string\":{\"
          analyze_wildcard\":true,\"query\":\"*\"}}}]}"
    }
  }
},
{
  "_id": "Crime-Servers",
  "_type": "dashboard",
  "_source": {
    "title": "Crime Servers",
    "hits": 0,
    "description": "",
    "panelsJSON": "[{\"col\":4,\"id\":\"Events-Map\",\"panelIndex\":1,\"row
        \":3,\"size_x\":6,\"size_y\":4,\"type\":\"visualization\"},{\"col
        \":10,\"id\":\"Top-10-Crime-Servers-by-Country\",\"panelIndex\":3,\"row
        \":3,\"size_x\":3,\"size_y\":4,\"type\":\"visualization\"},{\"col
        \":6,\"id\":\"Crime-Servers-Events\",\"panelIndex\":5,\"row\":11,\"
        size_x\":7,\"size_y\":4,\"type\":\"visualization\"},{\"col\":1,\"id
        \":\"TOP-10-C2\",\"panelIndex\":6,\"row\":3,\"size_x\":3,\"size_y
        \":4,\"type\":\"visualization\"},{\"col\":1,\"id\":\"ONLINE-
        CrimeServers\",\"panelIndex\":7,\"row\":1,\"size_x\":12,\"size_y\":2,\"
        type\":\"visualization\"},{\"id\":\"Top-10-C2-IPs\",\"type\":\"
        visualization\",\"panelIndex\":8,\"size_x\":5,\"size_y\":4,\"col\":1,\"
        row\":11},{\"id\":\"CrimeServers\",\"type\":\"visualization\",\"
        panelIndex\":9,\"size_x\":12,\"size_y\":4,\"col\":1,\"row\":7}]",
    "optionsJSON": "{\"darkTheme\":false}",
    "uiStateJSON": "{}",
    "version": 1,
    "timeRestore": true,
    "timeTo": "now/w",
    "timeFrom": "now/w",
    "kibanaSavedObjectMeta": {
      "searchSourceJSON": "{\"filter\":[{\"query\":{\"query_string\":{\"
          analyze_wildcard\":true,\"query\":\"*\"}}}]}"
    }
  }
},
{
  "_id": "Crime-Servers-Events",
  "_type": "visualization",
```

Blueliv.

```
  "_source"   {
   "title"    "Crime Servers Events"
   "visState"   "{\"type\":\"line\",\"params\":{\"shareYAxis\":true,\"
       addTooltip\":true,\"addLegend\":true,\"defaultYExtents\":false},\"aggs
       \":[{\"id\":\"1\",\"type\":\"count\",\"schema\":\"metric\",\"params
       \":{}},{\"id\":\"2\",\"type\":\"date_histogram\",\"schema\":\"segment
       \",\"params\":{\"field\":\"lastSeenAt\",\"interval\":\"day\",\"
       min_doc_count\":1,\"extended_bounds\":{}}},{\"id\":\"3\",\"type\":\"
       terms\",\"schema\":\"group\",\"params\":{\"field\":\"type.raw\",\"size
       \":5,\"order\":\"desc\",\"orderBy\":\"1\"}}],\"listeners\":{},\"title
       \":\"Crime Servers Events\"}"
   "uiStateJSON"   "{}"
   "description"   ""
   "version"   1
   "kibanaSavedObjectMeta"   {
     "searchSourceJSON"   "{\"index\":\"blueliv-crimeservers\",\"query\":{\"
         query_string\":{\"query\":\"*\",\"analyze_wildcard\":true}},\"filter
         \":[]}"
   }
  }
}
{
  "_id"   "Top-10-Crime-Servers-by-SubType"
  "_type"   "visualization"
  "_source"   {
   "title"    "Top 10 Crime Servers by SubType"
   "visState"   "{\"title\":\"Top 10 Crime Servers by Country\",\"type\":\"pie
       \",\"params\":{\"shareYAxis\":true,\"addTooltip\":true,\"addLegend\":
       true,\"isDonut\":false},\"aggs\":[{\"id\":\"1\",\"type\":\"count\",\"
       schema\":\"metric\",\"params\":{}},{\"id\":\"2\",\"type\":\"terms\",\"
       schema\":\"segment\",\"params\":{\"field\":\"subType.raw\",\"size
       \":10,\"order\":\"desc\",\"orderBy\":\"1\"}}],\"listeners\":{}}"
   "uiStateJSON"   "{}"
   "description"   ""
   "version"   1
   "kibanaSavedObjectMeta"   {
     "searchSourceJSON"   "{\"index\":\"blueliv-crimeservers\",\"query\":{\"
         query_string\":{\"query\":\"NOT subType:UNCLASSIFIED\",\"
         analyze_wildcard\":true}},\"filter\":[]}"
   }
  }
}
{
  "_id"   "Top-10-Crime-Servers-by-Country"
  "_type"   "visualization"
```

```
      "_source"   {
        "title"   "Top 10 Crime Servers by Country"
        "visState"   "{\"type\":\"pie\",\"params\":{\"shareYAxis\":true,\"addTooltip
            \":true,\"addLegend\":true,\"isDonut\":false},\"aggs\":[{\"id
            \":\"1\",\"type\":\"count\",\"schema\":\"metric\",\"params\":{}},{\"id
            \":\"2\",\"type\":\"terms\",\"schema\":\"segment\",\"params\":{\"field
            \":\"country.raw\",\"size\":10,\"order\":\"desc\",\"orderBy
            \":\"1\"}}],\"listeners\":{},\"title\":\"Top 10 Crime Servers by
            Country\"}"
        "uiStateJSON"   "{}"
        "description"   "",
        "version"   1
        "kibanaSavedObjectMeta"   {
          "searchSourceJSON"   "{\"index\":\"blueliv-crimeservers\",\"query\":{\"
              query_string\":{\"query\":\"*\",\"analyze_wildcard\":true}},\"filter
              \":[]}"
        }
      }
    }
    {
      "_id"   "Events-Map"
      "_type"   "visualization"
      "_source"   {
        "title"   "Events Map"
        "visState"   "{\"aggs\":[{\"id\":\"1\",\"params\":{},\"schema\":\"metric
            \",\"type\":\"count\"},{\"id\":\"2\",\"params\":{\"field\":\"location
            \",\"precision\":3},\"schema\":\"segment\",\"type\":\"geohash_grid
            \"}],\"listeners\":{},\"params\":{\"isDesaturated\":true,\"mapType\":\"
            Shaded Circle Markers\"},\"type\":\"tile_map\",\"title\":\"Events Map
            \"}"
        "uiStateJSON"   "{}"
        "description"   "",
        "version"   1
        "kibanaSavedObjectMeta"   {
          "searchSourceJSON"   "{\"index\":\"blueliv-crimeservers\",\"query\":{\"
              query_string\":{\"analyze_wildcard\":true,\"query\":\"*\"}},\"filter
              \":[]}"
        }
      }
    }
    {
      "_id"   "Bot-IP-per-hour"
      "_type"   "visualization"
      "_source"   {
        "title"   "Bot IP per hour"
```

Blueliv.

```
"visState" : "{\"title\":\"New Visualization\",\"type\":\"line\",\"params
    \":{\"shareYAxis\":true,\"addTooltip\":true,\"addLegend\":true,\"
    showCircles\":true,\"smoothLines\":false,\"interpolate\":\"linear\",\"
    scale\":\"linear\",\"drawLinesBetweenPoints\":true,\"radiusRatio\":9,\"
    times\":[],\"addTimeMarker\":false,\"defaultYExtents\":false,\"
    setYExtents\":false,\"yAxis\":{}},\"aggs\":[{\"id\":\"1\",\"type\":\"
    count\",\"schema\":\"metric\",\"params\":{}},{\"id\":\"2\",\"type\":\"
    date_histogram\",\"schema\":\"segment\",\"params\":{\"field\":\"seenAt
    \",\"interval\":\"h\",\"customInterval\":\"2h\",\"min_doc_count\":1,\"
    extended_bounds\":{}}}],\"listeners\":{}}"
"uiStateJSON" : "{}"
"description" : "",
"version" : 1,
"kibanaSavedObjectMeta" : {
  "searchSourceJSON" : "{\"index\":\"blueliv−ips\",\"query\":{\"query_string
      \":{\"query\":\"*\",\"analyze_wildcard\":true}},\"filter\":[]}"
}
}
}
{
  "_id" : "Top−10−Bot−IP",
  "_type" : "visualization",
  "_source" : {
    "title" : "Top 10 Bot IP",
    "visState" : "{\"title\":\"New Visualization\",\"type\":\"histogram\",\"
        params\":{\"shareYAxis\":true,\"addTooltip\":true,\"addLegend\":true,\"
        scale\":\"linear\",\"mode\":\"stacked\",\"times\":[],\"addTimeMarker\":
        false,\"defaultYExtents\":false,\"setYExtents\":false,\"yAxis\":{}},\"
        aggs\":[{\"id\":\"1\",\"type\":\"count\",\"schema\":\"metric\",\"params
        \":{}},{\"id\":\"2\",\"type\":\"terms\",\"schema\":\"segment\",\"params
        \":{\"field\":\"ip.raw\",\"size\":10,\"order\":\"desc\",\"orderBy
        \":\"1\"}}],\"listeners\":{}}"
    "uiStateJSON" : "{}"
    "description" : "",
    "version" : 1,
    "kibanaSavedObjectMeta" : {
      "searchSourceJSON" : "{\"index\":\"blueliv−ips\",\"query\":{\"query_string
          \":{\"query\":\"*\",\"analyze_wildcard\":true}},\"filter\":[]}"
    }
  }
}
{
  "_id" : "Top−10−Operating−Systems",
  "_type" : "visualization",
  "_source" : {
```

```
      "title"   "Top 10 Operating Systems"
      "visState"   "{\"title\":\"New Visualization\",\"type\":\"pie\",\"params
          \":{\"shareYAxis\":true,\"addTooltip\":true,\"addLegend\":true,\"
          isDonut\":false},\"aggs\":[{\"id\":\"1\",\"type\":\"count\",\"schema
          \":\"metric\",\"params\":{}},{\"id\":\"2\",\"type\":\"terms\",\"schema
          \":\"segment\",\"params\":{\"field\":\"operatingSystem.raw\",\"size
          \":10,\"order\":\"desc\",\"orderBy\":\"1\"}}],\"listeners\":{}}"
      "uiStateJSON"   "{}"
      "description"   ""
      "version"   1
      "kibanaSavedObjectMeta"   {
        "searchSourceJSON"   "{\"index\":\"blueliv−ips\",\"query\":{\"query_string
            \":{\"query\":\"*\",\"analyze_wildcard\":true}},\"filter\":[]}"
      }
    }
  }
}
{
   "_id"   "ONLINE−CrimeServers"
   "_type"   "visualization"
   "_source"   {
    "title"   "ONLINE CrimeServers"
    "visState"   "{\"title\":\"ONLINE CrimeServers\",\"type\":\"metric\",\"
        params\":{\"fontSize\":\"70\"},\"aggs\":[{\"id\":\"1\",\"type\":\"count
        \",\"schema\":\"metric\",\"params\":{}}],\"listeners\":{}}"
    "uiStateJSON"   "{}"
    "description"   ""
    "version"   1
    "kibanaSavedObjectMeta"   {
      "searchSourceJSON"   "{\"index\":\"blueliv−crimeservers\",\"query\":{\"
          query_string\":{\"query\":\"status:ONLINE\",\"analyze_wildcard\":true
          }},\"filter\":[]}"
    }
  }
}
{
   "_id"   "Botnet−URL"
   "_type"   "visualization"
   "_source"   {
    "title"   "Botnet URL"
    "visState"   "{\"title\":\"New Visualization\",\"type\":\"table\",\"params
        \":{\"perPage\":10,\"showPartialRows\":false,\"showMeticsAtAllLevels\":
        false},\"aggs\":[{\"id\":\"1\",\"type\":\"count\",\"schema\":\"metric
        \",\"params\":{}},{\"id\":\"2\",\"type\":\"terms\",\"schema\":\"bucket
        \",\"params\":{\"field\":\"botnetUrl.raw\",\"size\":10,\"order\":\"desc
        \",\"orderBy\":\"1\"}}],\"listeners\":{}}"
```

```
      "uiStateJSON"   "{}" ,
      "description"   "" ,
      "version"  1 ,
      "kibanaSavedObjectMeta"   {
        "searchSourceJSON"   "{\"index\":\"blueliv-ips\",\"query\":{\"query_string
            \":{\"query\":\"*\",\"analyze_wildcard\":true}},\"filter\":[]}"
      }
    }
  } ,
  {
    "_id"   "Top-10-Portal-domains" ,
    "_type"   "visualization" ,
    "_source"   {
      "title"   "Top 10 Portal domains" ,
      "visState"   "{\"title\":\"New Visualization\",\"type\":\"pie\",\"params
          \":{\"shareYAxis\":true,\"addTooltip\":true,\"addLegend\":true,\"
          isDonut\":false},\"aggs\":[{\"id\":\"1\",\"type\":\"count\",\"schema
          \":\"metric\",\"params\":{}},{\"id\":\"2\",\"type\":\"terms\",\"schema
          \":\"segment\",\"params\":{\"field\":\"portalDomain.raw\",\"size
          \":10,\"order\":\"desc\",\"orderBy\":\"1\"}}],\"listeners\":{}}" ,
      "uiStateJSON"   "{}" ,
      "description"   "" ,
      "version"  1 ,
      "kibanaSavedObjectMeta"   {
        "searchSourceJSON"   "{\"index\":\"blueliv-ips\",\"query\":{\"query_string
            \":{\"query\":\"*\",\"analyze_wildcard\":true}},\"filter\":[]}"
      }
    }
  } ,
  {
    "_id"   "Infection-Map" ,
    "_type"   "visualization" ,
    "_source"   {
      "title"   "Infection Map" ,
      "visState"   "{\"title\":\"New Visualization\",\"type\":\"tile_map\",\"
          params\":{\"mapType\":\"Scaled Circle Markers\",\"isDesaturated\":true
          ,\"addTooltip\":true,\"heatMaxZoom\":16,\"heatMinOpacity\":0.1,\"
          heatRadius\":25,\"heatBlur\":15,\"heatNormalizeData\":true,\"wms\":{\"
          enabled\":false,\"url\":\"https://basemap.nationalmap.gov/arcgis/
          services/USGSTopo/MapServer/WMSServer\",\"options\":{\"version
          \":\"1.3.0\",\"layers\":\"0\",\"format\":\"image/png\",\"transparent\":
          true,\"attribution\":\"Maps provided by USGS\",\"styles\":\"\"}}},\"
          aggs\":[{\"id\":\"1\",\"type\":\"count\",\"schema\":\"metric\",\"params
          \":{}},{\"id\":\"2\",\"type\":\"geohash_grid\",\"schema\":\"segment
          \",\"params\":{\"field\":\"location\",\"autoPrecision\":true,\"
```

```
            precision\":2}}],\"listeners\":{}}"
        "uiStateJSON"   "{}"
        "description"   ""
        "version"   1
        "kibanaSavedObjectMeta"   {
          "searchSourceJSON"   "{\"index\":\"blueliv-ips\",\"query\":{\"query_string
              \":{\"query\":\"*\",\"analyze_wildcard\":true}},\"filter\":[]}"
        }
      }
    }
    {
      "_id"   "TOP-10-C2"
      "_type"   "visualization"
      "_source"   {
        "title"   "Top 10 C2"
        "visState"   "{\n  \"aggs\": [\n    {\n      \"id\": \"1\",\n      \"params
            \": {},\n      \"schema\": \"metric\",\n      \"type\": \"count\"\n
            },\n    {\n      \"id\": \"2\",\n      \"params\": {\n        \"field
            \": \"subType.raw\",\n        \"order\": \"desc\",\n        \"orderBy
            \": \"1\",\n        \"size\": 10\n      },\n      \"schema\": \"segment
            \",\n      \"type\": \"terms\"\n    }\n  ],\n  \"listeners\": {},\n  \"
            params\": {\n    \"addLegend\": true,\n    \"addTooltip\": true,\n
            \"isDonut\": false,\n    \"shareYAxis\": true\n  },\n  \"title\": \"New
             Visualization\",\n  \"type\": \"pie\"\n}"
        "uiStateJSON"   "{}"
        "description"   ""
        "version"   1
        "kibanaSavedObjectMeta"   {
          "searchSourceJSON"   "{\n  \"index\": \"blueliv-crimeservers\",\n  \"query
              \": {\n    \"query_string\": {\n      \"query\": \"type:C_AND_C\",\n
                  \"analyze_wildcard\": true\n    }\n  },\n  \"filter\": []\n}"
        }
      }
    }
    {
      "_id"   "CrimeServers"
      "_type"   "visualization"
      "_source"   {
        "title"   "CrimeServers"
        "visState"   "{\"title\":\"New Visualization\",\"type\":\"table\",\"params
            \":{\"perPage\":10,\"showMeticsAtAllLevels\":false,\"showPartialRows\":
            false},\"aggs\":[{\"id\":\"1\",\"type\":\"count\",\"schema\":\"metric
            \",\"params\":{}},{\"id\":\"2\",\"type\":\"terms\",\"schema\":\"bucket
            \",\"params\":{\"field\":\"url.raw\",\"size\":10,\"order\":\"desc\",\"
            orderBy\":\"_term\"}},{\"id\":\"3\",\"type\":\"terms\",\"schema\":\"
```

```
        bucket\",\"params\":{\"field\":\"type.raw\",\"size\":10,\"order\":\"
        desc\",\"orderBy\":\"_term\"}},{\"id\":\"4\",\"type\":\"terms\",\"
        schema\":\"bucket\",\"params\":{\"field\":\"status.raw\",\"size\":10,\"
        order\":\"desc\",\"orderBy\":\"_term\"}},{\"id\":\"5\",\"type\":\"terms
        \",\"schema\":\"bucket\",\"params\":{\"field\":\"ip.raw\",\"size\":5,\"
        order\":\"desc\",\"orderBy\":\"_term\"}},{\"id\":\"6\",\"type\":\"terms
        \",\"schema\":\"bucket\",\"params\":{\"field\":\"lastSeenAt\",\"size
        \":10,\"order\":\"desc\",\"orderBy\":\"1\"}}],\"listeners\":{}}",
      "uiStateJSON"   "{}",
      "description"   "",
      "version"   1,
      "kibanaSavedObjectMeta"   {
        "searchSourceJSON"   "{\"index\":\"blueliv-crimeservers\",\"query\":{\"
            query_string\":{\"query\":\"*\",\"analyze_wildcard\":true}},\"filter
            \":[]}"
      }
    }
  },
  {
    "_id"   "Top-10-C2-IPs",
    "_type"   "visualization",
    "_source"   {
      "title"   "Top 10 C2 IPs",
      "visState"   "{\"title\":\"New Visualization\",\"type\":\"histogram\",\"
          params\":{\"shareYAxis\":true,\"addTooltip\":true,\"addLegend\":true,\"
          scale\":\"linear\",\"mode\":\"stacked\",\"times\":[],\"addTimeMarker\":
          false,\"defaultYExtents\":false,\"setYExtents\":false,\"yAxis\":{}},\"
          aggs\":[{\"id\":\"1\",\"type\":\"count\",\"schema\":\"metric\",\"params
          \":{}},{\"id\":\"2\",\"type\":\"terms\",\"schema\":\"segment\",\"params
          \":{\"field\":\"ip.raw\",\"size\":10,\"order\":\"desc\",\"orderBy
          \":\"1\"}}],\"listeners\":{}}",
      "uiStateJSON"   "{}",
      "description"   "",
      "version"   1,
      "kibanaSavedObjectMeta"   {
        "searchSourceJSON"   "{\"index\":\"blueliv-crimeservers\",\"query\":{\"
            query_string\":{\"analyze_wildcard\":true,\"query\":\"type:C_AND_C
            \"}},\"filter\":[]}"
      }
    }
  }
]
```

Listing 3.3: Kibana dashboards example

You can find these dashboards at our GitHub.

3.6.1 Example Dashboards

Here you can find two example Dashboards (3.3): BotIPs and CrimeServers. Please be aware that these dashboards will only work if you set-up the indexes like we explained in listing 3.1. Otherwise you need to create them yourself.

Blueliv.

Registration

If you are interested in getting full access to our Threat Intelligence feed, contact us via email to get your API credentials that will allow you to update your local Data Base with current and real-time Threat Intelligence updates.

There are two access modes, Commercial and Free. If you are using the Free access, you will not have access to all the data we offer.

Blueliv.

23
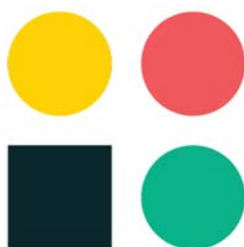
IMPROVE YOUR CYBER THREAT VISIBILITY

info@blueliv.com   www.blueliv.com