


Sécurité et visualisation des données



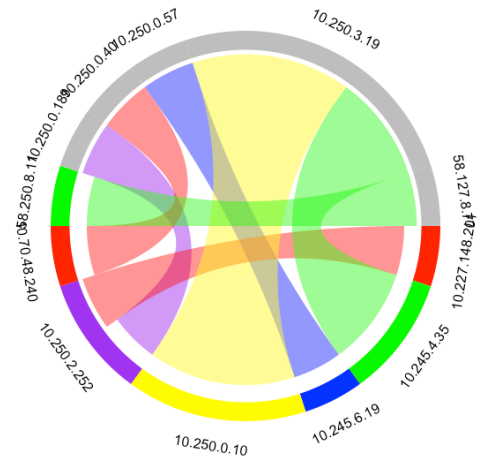
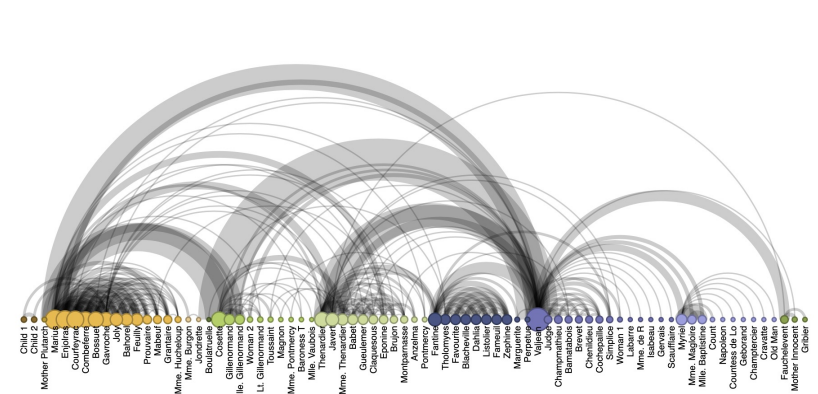
TD FreeStyle : mode graphique

- Préparation pour le challenge
 - Données issues d'un Firewall Iptables/Apache
 - Champs prédécoupés par un template Syslog-ng (patterndb)
 - Données à traiter en R/Python
 - Analyse descriptive simple (TOP 10 Ipsrc, Ipdst, protocoles utilisés)

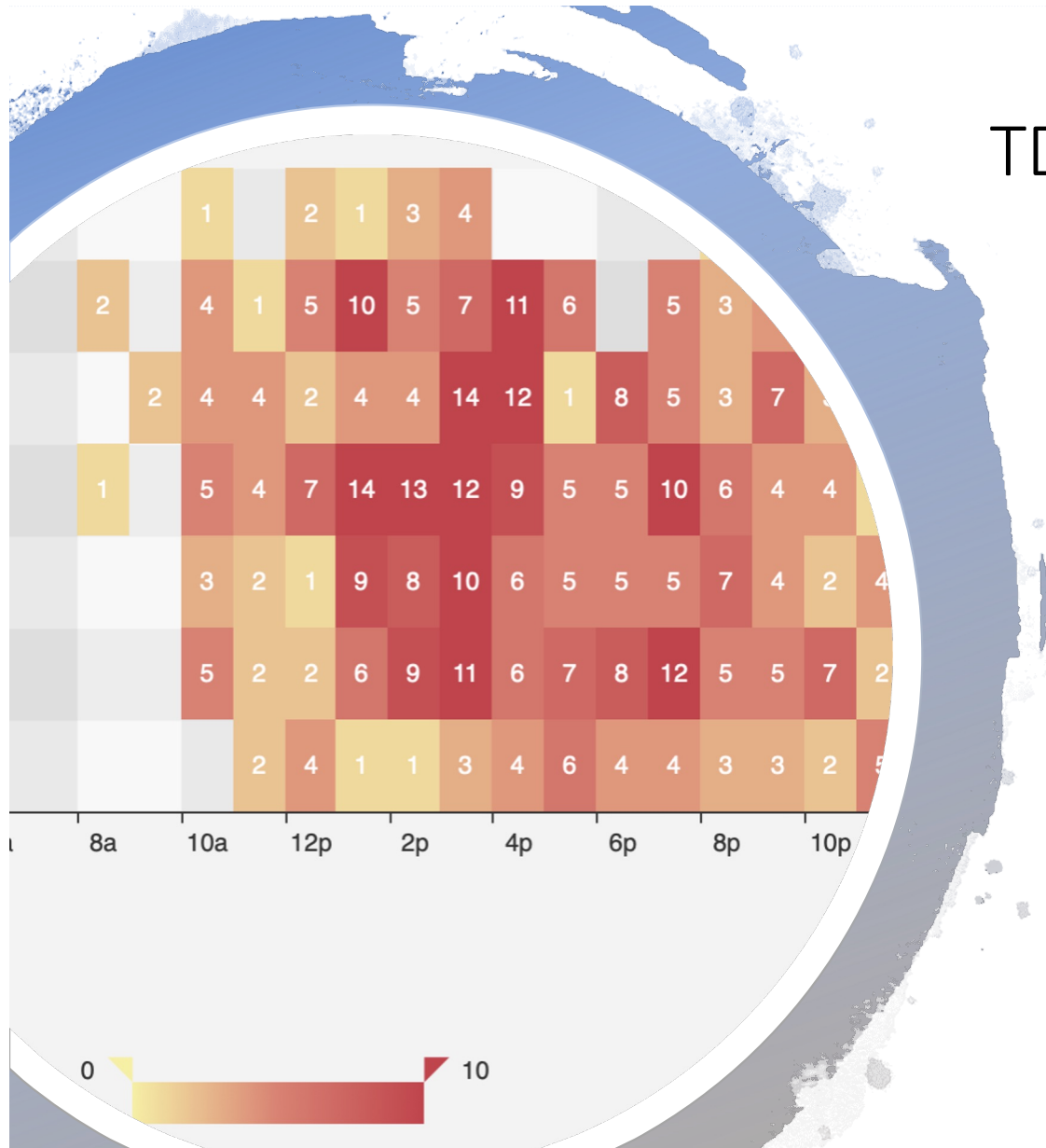


TD FreeStyle : mode graphique

- Lien [graph](https://rpubs.com/matungawalla/circular_matrix) 1 : https://rpubs.com/matungawalla/circular_matrix
- Lien [graph](https://www.r-bloggers.com/arc-diagrams-in-r-les-miserables/) 2 : <https://www.r-bloggers.com/arc-diagrams-in-r-les-miserables/>



TD FreeStyle : mode graphique



Lien [graph](https://www.echartsjs.com/en/index.html) 3 : <https://www.echartsjs.com/en/index.html>

TD FreeStyle : Rshiny

Noms-Prenoms-Groupe

Protocole :

☒ TCP

☐ UDP

☐ TCP & UDP

Ports :

☒ Inferieur 1024

☐ Superieur 1024

☐ Tous les ports

Se balader dans Parcourir

1 149

1 16 31 46 61 76 91 106 121 136 149

Nombre de classes

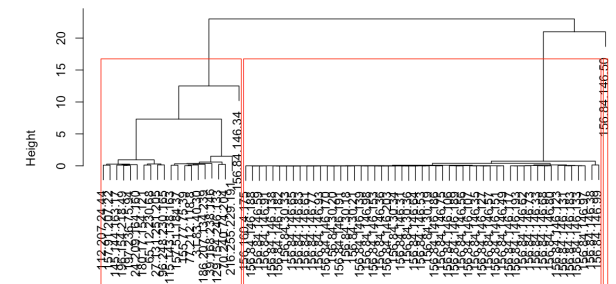
3

☐ Inertie pour CAH

[Synthese des flux](#) [Visualisation donnees brutes](#) [Parcourir](#)

CAH sur serveur principal

Vue globale



IP Source
Agglomerative Coefficient = 0.98

The slide features a solid orange background. A large white circle is centered on the slide. The text "Intro ELK" is written in orange inside the white circle. On the left side of the white circle, there is a dashed yellow arc. On the bottom right edge of the white circle, there is a small solid blue circle.

Intro ELK

The logo features the letters 'ELK' in a white, bold, sans-serif font. Above the letters is a yellow dashed arc. To the left of the letters is a solid yellow circle. To the right is a yellow square outline. The entire logo is set against a solid orange rectangular background.

ELK

- Trois composants forment une solution puissante pour la collecte, le stockage, la recherche et l'analyse des logs et d'autres types de données.
- ELK est largement utilisé dans divers domaines, tels que le monitoring des applications, la sécurité informatique, l'analyse des performances système, et bien plus encore.

3

composants

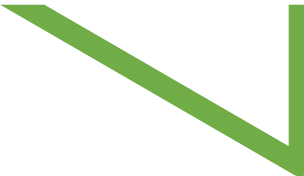
Elasticsearch: Il s'agit d'un moteur de recherche et d'analyse distribué, conçu pour stocker, rechercher et analyser de grandes quantités de données en temps réel. Elasticsearch est particulièrement efficace pour effectuer des recherches textuelles complexes, des agrégations et des analyses de données.

Logstash: Logstash est un outil de traitement des logs qui permet d'ingérer, de traiter et de transformer des données de différents formats et sources avant de les envoyer à Elasticsearch pour l'indexation et l'analyse. Il est souvent utilisé pour normaliser les logs provenant de sources hétérogènes.

Kibana: Kibana est une interface utilisateur web qui permet de visualiser et d'analyser les données stockées dans Elasticsearch. Elle offre des fonctionnalités de création de tableaux de bord, de visualisations graphiques et de recherche de données. Kibana permet aux utilisateurs de mieux comprendre leurs données et de prendre des décisions informées à partir des insights obtenus.



Lancement

- 
- Builder les conteneurs (docker build -t elas-sise .)
 - docker run -itd --privileged -p 9300:9300 -p 9200:9200 --name e-sis elas-sise
 - docker run -itd --privileged -p 5601:5601 --name kib-sise kibans-sise
 - Docker ps -a

Modification

`docker exec -it kib-sise bash`

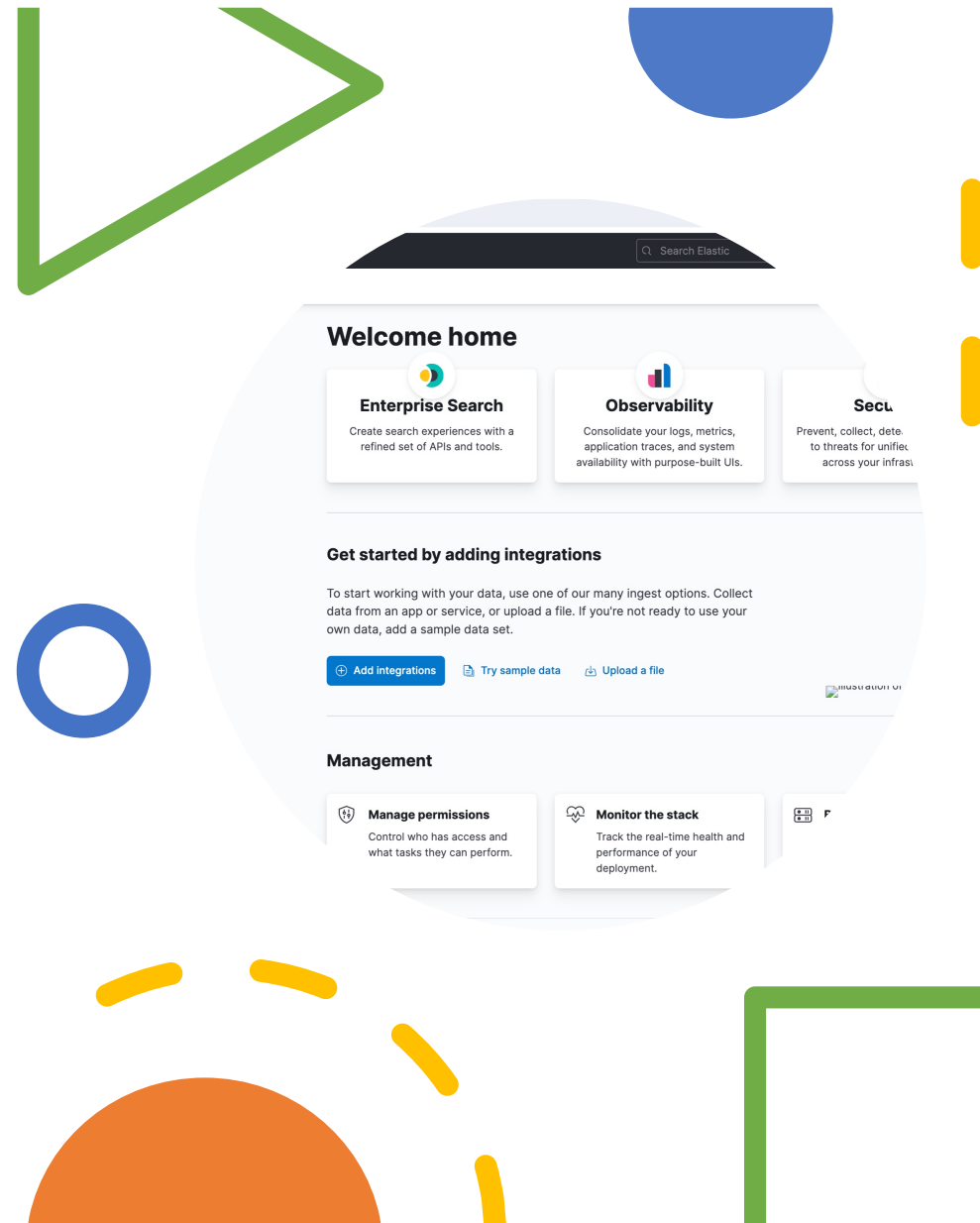
Editer le fichier `/etc/kibana/kibana.yml`

Modifier la ligne `elasticsearch.hosts`: inclure l'adresse du conteneur Elastic (`docker inspect e-sis`)

Relancer Kibana (`service kibana restart`)

Tests de connexion

- Test de connexion Elastic : <http://localhost:9200>
- Accès à Kibana : <http://localhost:5601>



Demo et tests

Kibana

Graph & Dashboard

Logstash



Focus sur Logstash E/S:

- Logstash -f export.conf

```
input {  
  stdin { }  
}  
output {  
  file {  
    path => "./opsie.txt"  
  }  
  elasticsearch {  
    action => "index"  
    index => "iptables"  
  }  
  stdout {}  
}
```

```
input {  
  udp{  
    port=>514  
    type => "network"  
  }  
}
```

Exemple de filtre

```
filter {  
  csv {  
    separator => ";"  
    columns => ["Fin du controle", "Gare - Code UIC", "Gare", "Nombre  
observations", "Nombre de Non Conformites"]  
  }  
  mutate {  
    remove_field => [ "message", "path" , "@version", "@timestamp",  
"host"]  
  }  
}
```

Fichier source :

```
2023-03-21T12:03:00+01:00;0087396002;Le Mans;88.0;5.0  
2023-03-21T12:06:00+01:00;0087751008;Marseille Saint-Charles;89.0;13.0  
2023-03-21T12:10:00+01:00;0087784009;Perpignan;76.0;4.0  
2023-03-21T12:34:00+01:00;0087582825;Saint-Macaire;21.0;3.0  
2023-03-21T12:43:00+01:00;0087582734;Podensac;39.0;4.
```



Logstash : filter

```
filter {  
  grok {  
    match => {  
      "message" => "%{DATA:trim}  
%{DATA:base} %{DATA:user} %{DATA:divers}"  
    }  
  }  
}
```

- Sympa et à voir : <https://grokdebugger.com>
- 
- 



```
input {
  udp {
    port => 514
    type => "network"
    tags => ["serverweb_kali"]
  }
}
filter {
  if "serverweb_kali" in [tags]{
    grok {
      match => {"message" => "%{SYSLOGTIMESTAMP:timestamp}
%{SYSLOGHOST:sysloghost} kernel: \[%{DATA:kern}\] %{DATA:action} RULE=%{INT:rule}
IN=%{DATA:in} OUT=%{DATA:} MAC=%{DATA:mac} SRC=%{IPV4:srcip} DST=%{IPV4:dstip}
%{DATA:} PROTO=%{WORD:proto} SPT=%{INT:src_port} DPT=%{INT:dst_port}"
    }
  }
}
mutate{
  remove_field => ["sysloghost","kern","timestamp"]
}
}
output {
  file {
    path => "./d.txt"
  }
  elasticsearch {
    action => "index"
    index => "tsyslog"
  }
  stdout {}
}
```



A large orange rounded rectangle on the left side of the slide.

Différentes
sources

- Logstash
- Metricbeat
- Filebeat





Exemple d'OUTPUT

```
output {  
  if "apache2" in [tags]{  
    file {      path => "./d.txt"  
    }  
    stdout {}  
  }  
  elasticsearch {  
    action => "index"  
    index => "tsyslog »"  
    hosts => ["https://mon_ip:9200"]  
  }  
  if "serverweb_kali" in [tags]{  
    file {      path => "./f.txt"  
    }  
    stdout {}  
  }  
}
```

