FCCN UNIDADE DA FCT
Tecnologia para o Conhecimento

CSIRT IN A BOX 2022

SIEM

Pedro Silva

RCTS CERT

CERT RCTS

AGENDA

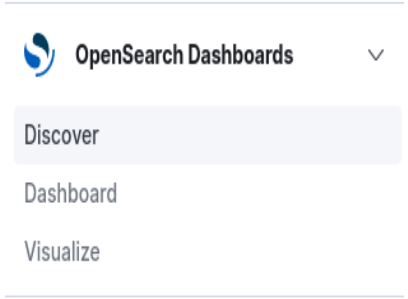
- Introdução
- Parte teórica
- Parte prática
- Resultados

INTRODUÇÃO

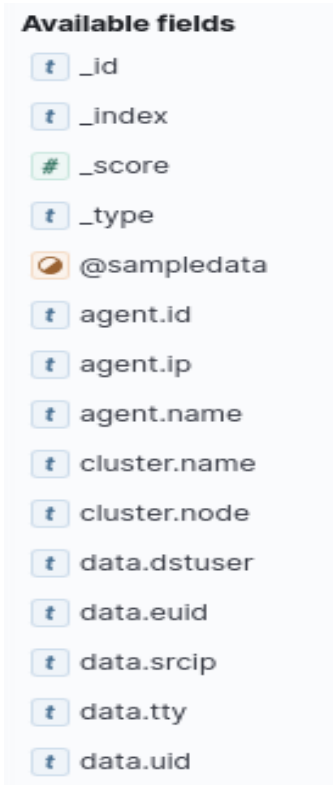

Log Collection
Log Analysis
Event Correlation
Log Forensics
IT Compliance
Application Log Monitoring
Object Access Auditing
SIEM
Real-time Alerting
User Activity Monitoring
Dashboards
Reporting
File Integrity Monitoring
System & Device Log Monitoring
Log Retention

PARTE TEÓRICA

Descobrir

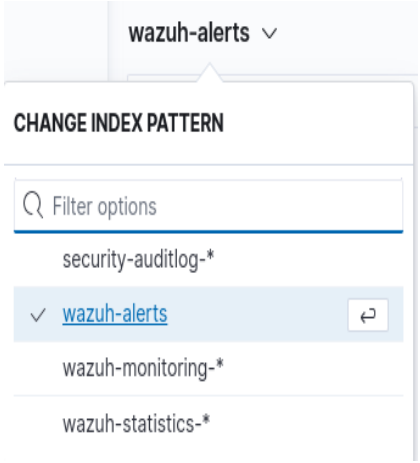


Campos

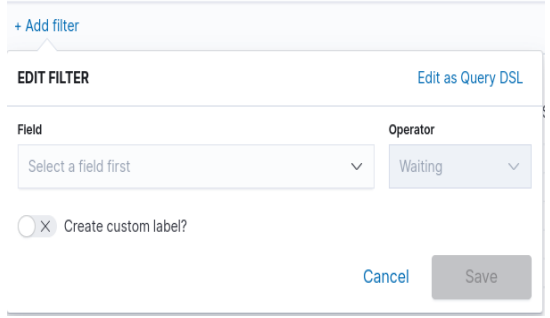


Data

Indexes



Filtros



FCCN UNIDADE DA FCT

Fundação para a Ciência e a Tecnologia

PARTE PRÁTICA
URL:
USERNAME:
PASSWORD:

1. Quantas tentativas de autenticação sem sucesso aconteceram provenientes do IP 141.98.81.37 (ssh)?

2. A equipa de segurança precisa de saber qual o nome do(s) ficheiro(s) usados no comando onde foram elevados os privilégios (sudo)?

3. Quais os IPs que comunicaram, usando o protocolo HTTP, com o servidor "Ubuntu", cujo agente é um iphone?

(15 minutos)

O tempo terminou

RESULTADOS 1

- 38 tentativas

```
{
  "query": {
    "match_phrase": {
      "full_log": "authentication failure"
    }
  }
}
```

```
{
  "query": {
    "match_phrase": {
      "data.srcip": "141.98.81.37"
    }
  }
}
```

GOAL: usar filtros para capturar a informação desejada.

RESULTADOS 2

- /etc/sample/file

```
{
  "query": {
    "match_phrase": {
      "data.audit.command": "sudo"
    }
  }
}
```

GOAL: usar um filtro para captar grande parte da informação desejada e usar os campos para visualizar apenas o que precisamos

RESULTADOS 3

- 45.124.37.241
- 187.80.4.18
- 141.98.81.37
- 40.220.102.15
- 45.75.196.15
- 134.87.21.47
- 54.10.24.5

```
{
 "query": {
  "match_phrase": {
   "full_log": "GET / HTTP"
  }
 }
}
```

```
{
 "query": {
  "bool": {
   "must": [
    {
     "match_phrase": {
      "full_log": "iPhone"
     }
    }
   ]
  }
 }
}
```

GOAL: usar vários filtros, ou 1 filtro mais complexo, criados faseadamente à medida das necessidades, neste caso sistema operativos preteridos, de seguida pedir para visualizar.

Obrigado!