**ES文档设计**

目录

[概述： 2](#_Toc499048804)

[系统组织图： 2](#_Toc499048805)

[文档设计： 3](#_Toc499048806)

[1、威胁事件文档，mapping如下 3](#_Toc499048807)

[1、一个来自surveyor的威胁事件，文档内容示例： 4](#_Toc499048808)

[2、一个来自digger的异常流量检查的威胁事件，文档内容示例： 5](#_Toc499048809)

[2、资产流量统计文档，mapping如下： 5](#_Toc499048810)

[1、文档内容示例： 6](#_Toc499048811)

[3、行为告警文档，mapping如下： 7](#_Toc499048812)

[1、一个由minerva产生的告警事件，文档内容示例： 8](#_Toc499048813)

[2、一个由digger产生的告警事件，文档内容示例： 9](#_Toc499048814)

# 概述：

对系统中数据量比较大的模块，初步设计了其文档组织，分为3个index，包括：

1、events

2、statistics

3、behavior

每一个index下对应的type可以用时间确定，类似分表的方式，如2017或者201701，表示2017年或者2017年1月的数据（当然，如果性能满足，可以将以上3个index作为type，统一存在一个index下）。

如：

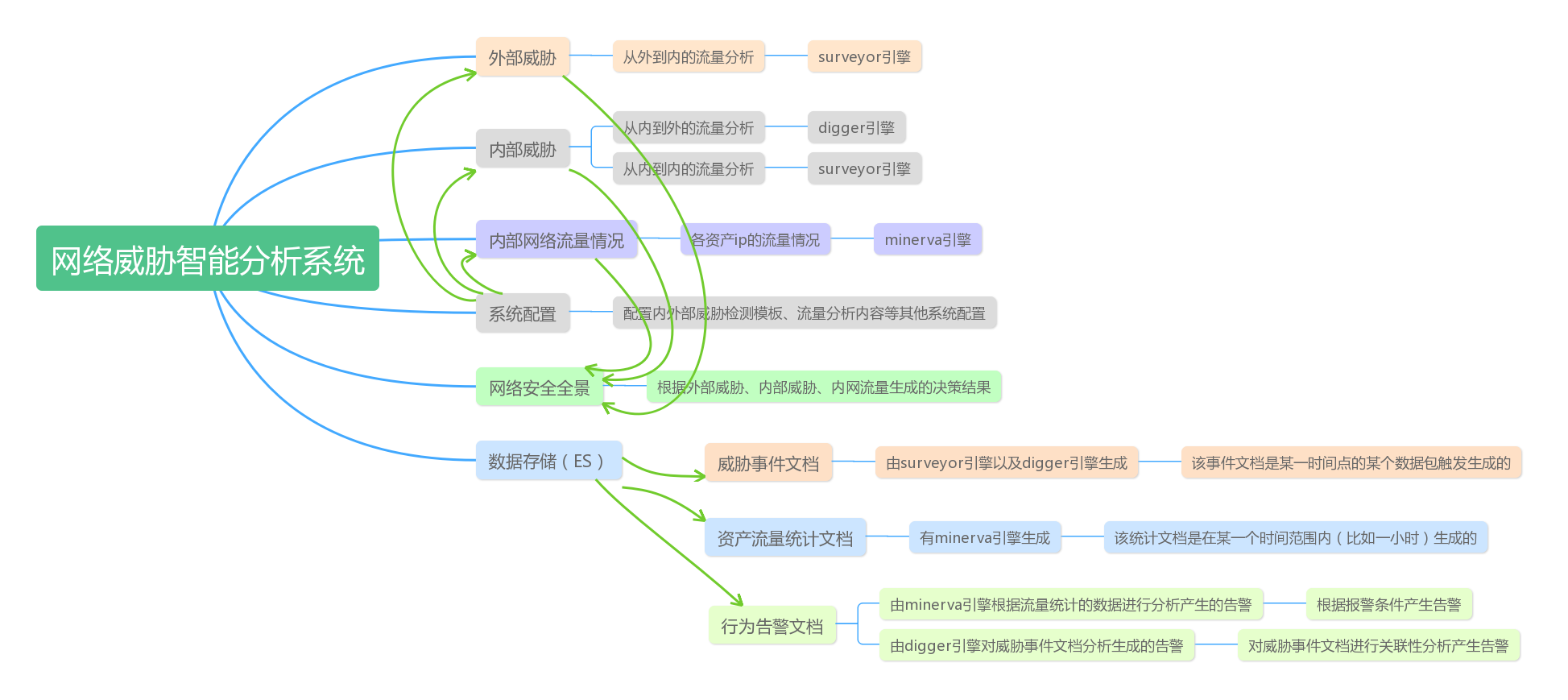
/events/2017/docx || /event/201701/docx || /es/events/docx

/statistics/2017/docx || / statistics /201701/docx || /es/ statistics /docx

/ behavior /2017/docx || / behavior /201701/docx || /es/ behavior /docx

具体使用方式可根据数据量大小确定。

# 系统组织图：



# 文档设计：

## 1、威胁事件文档，mapping如下

curl -XPUT localhost:9200/events?pretty -d '{

"mappings":{

"\_default\_":{

"properties":{

"property\_ip":{ //资产ip

"type":"ip"

},

"remote\_ip":{ //外部ip

"type":"ip"

},

"property\_port":{ //资产端口

"type":"short"

},

"remote\_port":{ //外部端口

"type":"short",

"index":"false"

},

"protocol":{ //传输层协议

"type":"keyword"

},

"event\_type":{ //事件类型

"type":"keyword"

},

"signature":{ //事件特征

"type":"keyword",

"index":"false"

},

"app\_proto":{ //应用层协议

"type":"keyword"

},

"level":{ //事件等级 deadly，critical，normal，low-risk，suspicious

"type":"keyword"

},

"rule\_id":{ //匹配的规则id

"type":"keyword",

"index":"false"

},

"status":{ //事件状态，成功与否

"type":"short"

},

"handled":{ //处置标志，是否处置

"type":"short"

},

"advisement":{ //建议

"type":"keyword"

},

"source":{ //事件来源，外部的威胁还是内部的威胁

"type":"keyword"

},

"pkt\_data":{ //数据包，数组

"type":"nested"

},

"timestamp":{ //时间

"type":"date",

"format": "yyyy-MM-dd HH:mm:ss||yyyy-MM-dd||epoch\_millis"

}

}

}

}

}'

### 1、一个来自surveyor的威胁事件，文档内容示例：

curl -XPOST 'localhost:9200/events/2017/' -d '{

"property\_ip":"192.168.2.111",

"remote\_ip":"154.2.39.23",

"property\_port":80,

"remote\_port":13259,

"protocol":"tcp",

"event\_type":"browser-attack",

"signature":"BROWSER-FIREFOX Mozilla multiple content-length headers malicious redirect attempt",

"app\_proto":"http",

"level":"normal",

"rule\_id":20585,

"status":0，

"handled":0,

"advisement":"请下载最新版本的浏览器，并使用杀毒软件进行全面杀毒",

"source":"surveyor",

"pkt\_data":[

{

"timestamp":"2017-11-11 11:11:11",

"data":"xxxxxxxxxxxxxxxxxxxxxxxx"

},

{

"timestamp":"2017-11-11 11:11:12",

"data":"yyyyyyyyyyyyyyyyyyyyyyyy"

}

],

"timestamp":"2017-11-11 11:11:11"

}'

### 2、一个来自digger的异常流量检查的威胁事件，文档内容示例：

curl -XPOST 'localhost:9200/events/2017/' -d '{

"property\_ip":"192.168.2.112",

"remote\_ip":"158.2.54.13",

"property\_port":8080,

"remote\_port":13559,

"protocol":"tcp",

"event\_type":"suspicious-domain", 可疑域名

"signature":"www.igotyou.com.cn",

"app\_proto":"dns",

"level":"critical",

"rule\_id":0,

"status":0，

"handled":0,

"advisement":"请检查资产ip为192.168.2.112的设备是否正常，并扫描是否存在恶意软件",

"source":"digger",

"pkt\_data":[

{

"timestamp":"2017-11-11 11:11:11",

"data":"xxxxxxxxxxxxxxxxxxxxxxxx"

}

],

"timestamp":"2017-11-11 11:11:11"

}'

## 2、资产流量统计文档，mapping如下：

curl -XPUT localhost:9200/statistics?pretty -d '{

"mappings":{

"\_default\_":{

"properties":{

"property\_ip":{ //资产ip

"type":"ip"

},

"protocol":{ //传输层协议

"type":"nested"

},

"port":{ //事件类型

"type":"nested"

},

"zone":{ //事件特征

"type":"nested"

},

"timestamp":{ //时间

"type":"date",

"format": "yyyy-MM-dd HH:mm:ss||yyyy-MM-dd||epoch\_millis"

}

}

}

}

}'

### 1、文档内容示例：

curl -XPOST 'localhost:9200/statistics/2017/' -d '{

"property\_ip":"192.168.2.112",

"timestamp":"2017-11-11 11",

"protocol":[

{

"proto":"tcp",

"up\_cnt":100,

"up\_bytes":29130,

"down\_cnt":39023,

"down\_bytes":409012

},

{

"proto":"udp",

"up\_cnt":100,

"up\_bytes":29130,

"down\_cnt":39023,

"down\_bytes":409012

}

],

"ports":[

{

"port":"80",

"up\_cnt":100,

"up\_bytes":29130,

"down\_cnt":39023,

"down\_bytes":409012

},

{

"port":"23",

"up\_cnt":100,

"up\_bytes":29130,

"down\_cnt":39023,

"down\_bytes":409012

}

],

"zone":[

{

"region":"usa",

"up\_cnt":100,

"up\_bytes":29130,

"down\_cnt":39023,

"down\_bytes":409012

},

{

"region":"cd",

"up\_cnt":100,

"up\_bytes":29130,

"down\_cnt":39023,

"down\_bytes":409012

}

]

}'

## 3、行为告警文档，mapping如下：

curl -XPUT localhost:9200/behavior?pretty -d '{

"mappings":{

"\_default\_":{

"properties":{

"ip":{ //触发告警的ip

"type":"ip"

},

"event\_type":{ //事件类型

"type":"keyword"

},

"signature":{ //事件特征

"type":"keyword",

"index":"false"

},

"criteria":{ //判定依据

"type":"keyword"

},

"algorithm":{ //判定算法

"type":"keyword"

},

"level":{ //事件等级 deadly，critical，normal，low-risk，suspicious

"type":"keyword"

},

"handled":{ //处置标志，是否处置

"type":"short"

},

"advisement":{ //建议

"type":"keyword"

},

"source":{ //事件来源，外部的威胁还是内部的威胁

"type":"short"

},

"timestamp":{ //时间

"type":"date",

"format": "yyyy-MM-dd HH:mm:ss||yyyy-MM-dd||epoch\_millis"

}

}

}

}

}'

### 1、一个由minerva产生的告警事件，文档内容示例：

curl -XPOST 'localhost:9200/ behavior /2017/' -d '{

"property\_ip":"192.168.2.113",

"event\_type":"会话异常",

"signature":"小包个数占比太多",

"criteria":"在一段时间内，该资产ip的会话流量符合木马通信的特征",

"algorithm":"行为分析算法",

"level":"suspicious",

"status":0，

"handled":0,

"advisement":"请检查资产ip为192.168.2.112的设备是否正常，并扫描是否存在恶意软件",

"source":"minerva",

"timestamp":"2017-11-11 11:11:11"

}'

### 2、一个由digger产生的告警事件，文档内容示例：

curl -XPOST 'localhost:9200/behavior /2017/' -d '{

"ip":"158.98.123.22",

"event\_type":"疑似攻击",

"signature":"数据包持续匹配规则",

"criteria":"在一段时间内，该外部ip持续对资产进行试探攻击",

"algorithm":"行为分析算法",

"level":"suspicious",

"status":0，

"handled":0,

"advisement":"请检查158.98.123.22的ip是否有可疑记录，并将该ip加入防火墙",

"source":"digger",

"timestamp":"2017-11-11 11:11:11"

}'