Elasticsearch在移动病毒侦测领域应用那些事儿

Mobile Threat Response Team

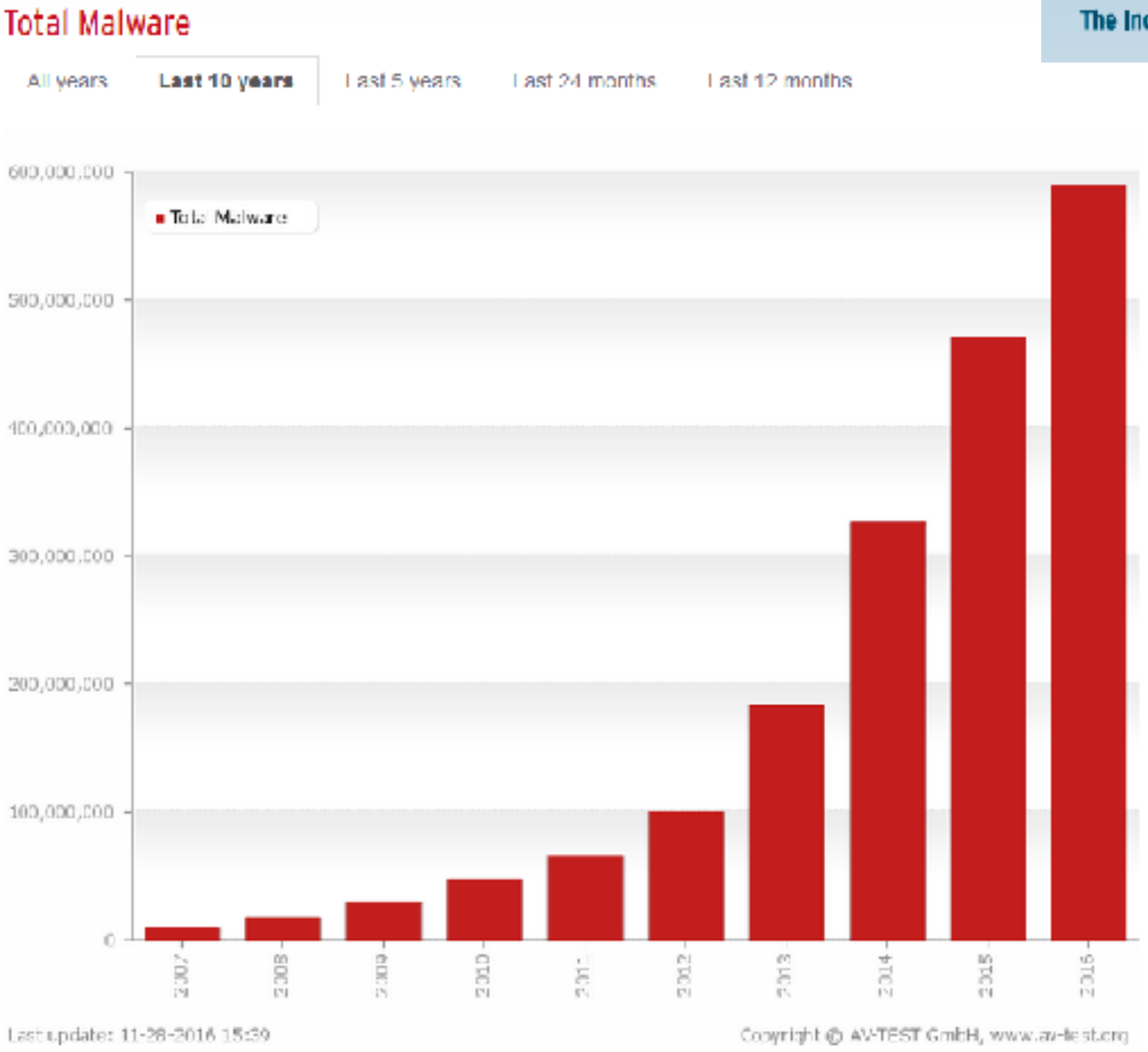
李啸（White Li）

关于我

- 李啸（White Li）.
- 百度，小米，华为南研（SRE、Developer）
- 趋势科技（ Senior Developer /Ops ）
- 移动专家系统开发（android/mac/ios）
- white_li@trendmicro.com.cn
- https://github.com/swordsmanli
- Based in Nanking.

移动病毒激增

AV-TEST
The Independent IT-Security Institute
Magdeburg Germany



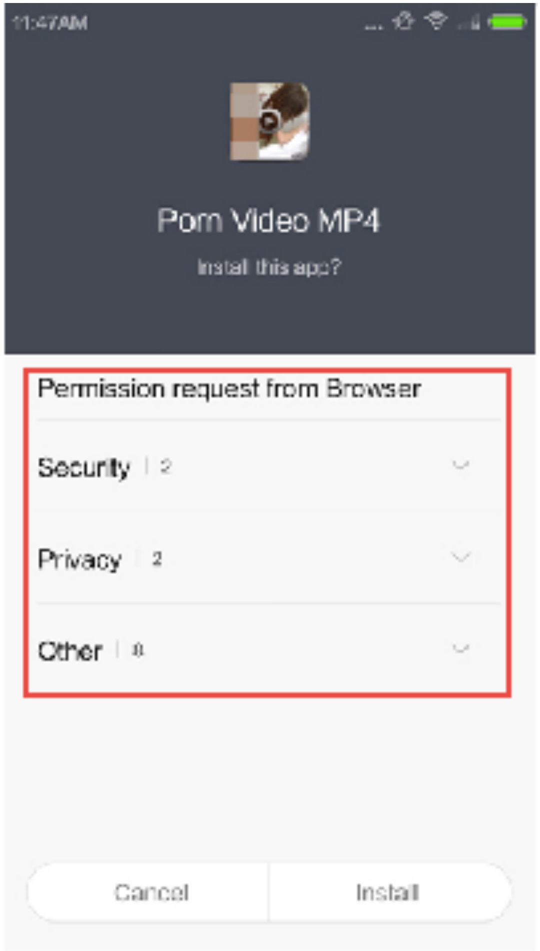
TREND MICRO

话题

- **移动病毒特征与Elasticsearch**
- 病毒长啥样
- 权限模型简介
- 危险的权限
- 病毒特征(提取，存储，查询)
- Elasticsearch引擎
- 分集群存储
- 集群数据

- **Predator**
- 烦人的DSL
- 多表联合查询
- Threat Inteligence

一个ransomware病毒



11:47AM

Porn Video MP4

Install this app?

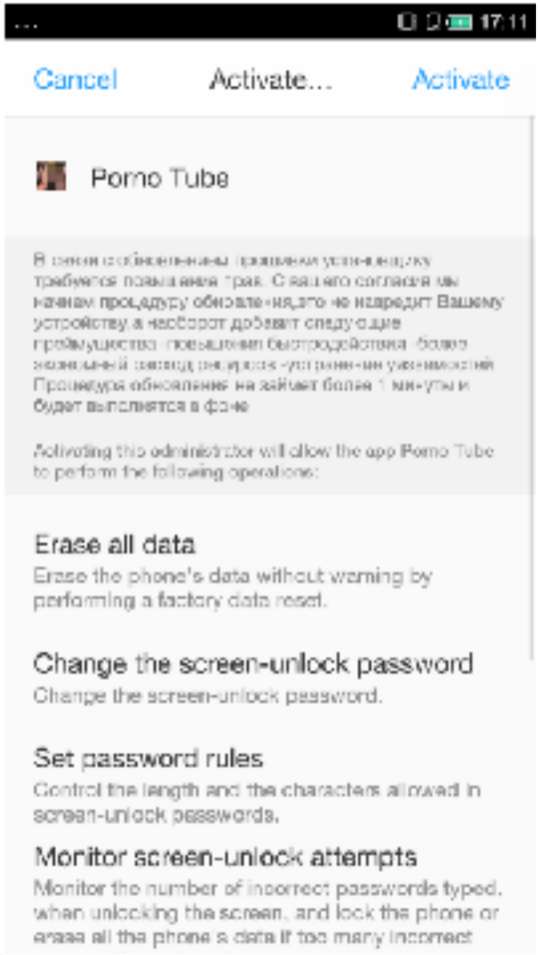
Permission request from Browser

Security | 2

Privacy | 2

Other | 8

Cancel | Install



17:11

Cancel Activate... Activate

Porno Tube

В связи с обнаруженными проблемами установщику требуется повышение прав. С вашего согласия мы начнем процедуру обновления,это не навредит Вашему устройству,а наоборот добавит следующие преймущества: повышение быстродействия, более экономный расход ресурсов, устранение уязвимостей. Процедура обновления не займет более 1 минуты и будет выполнятся в фоне

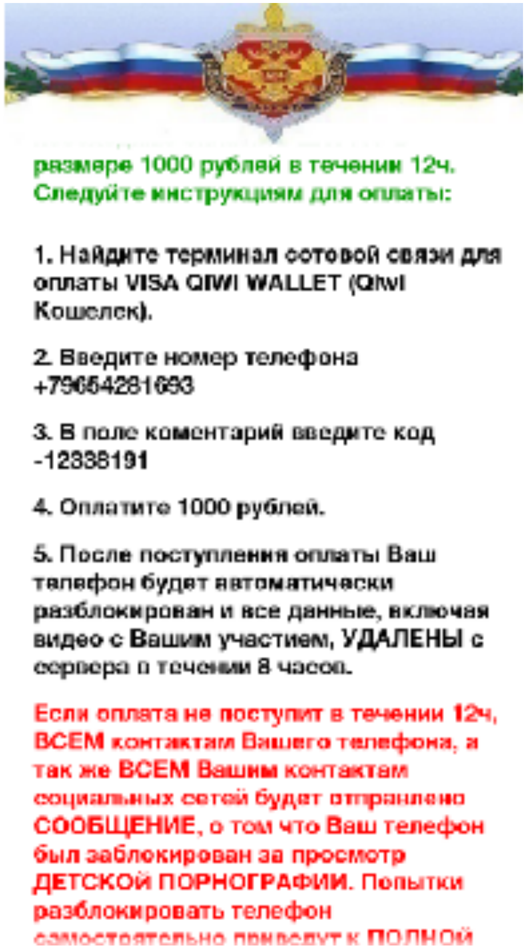
Activating this administrator will allow the app Porno Tube to perform the following operations:

Erase all data
Erase the phone's data without warning by performing a factory data reset.

Change the screen-unlock password
Change the screen-unlock password.

Set password rules
Control the length and the characters allowed in screen-unlock passwords.

Monitor screen-unlock attempts
Monitor the number of incorrect passwords typed. when unlocking the screen, and lock the phone or erase all the phone's data if too many incorrect



размере 1000 рублей в течении 12ч.
Следуйте инструкциям для оплаты:

1. Найдите терминал сотовой связи для оплаты VISA QIWI WALLET (Qiwi Кошелек).

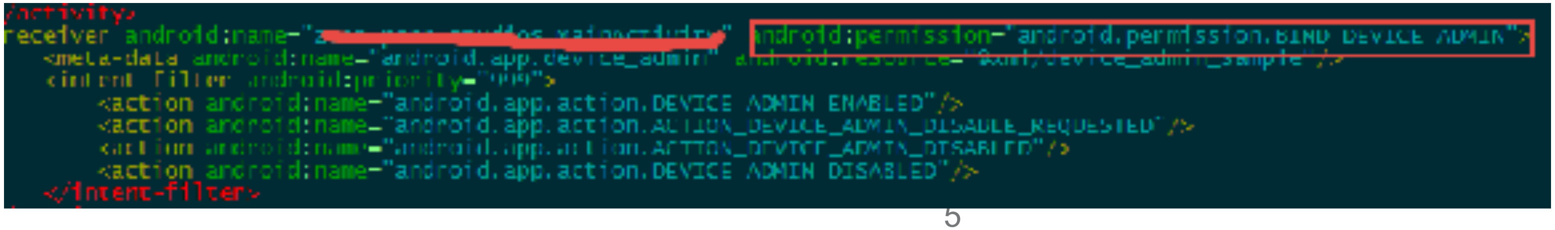
2. Введите номер телефона +79654281693

3. В поле коментарий введите код -12338191

4. Оплатите 1000 рублей.

5. После поступления оплаты Ваш телефон будет автоматически разблокирован и все данные, включая видео с Вашим участием, УДАЛЕНЫ с сервера в течении 8 часов.

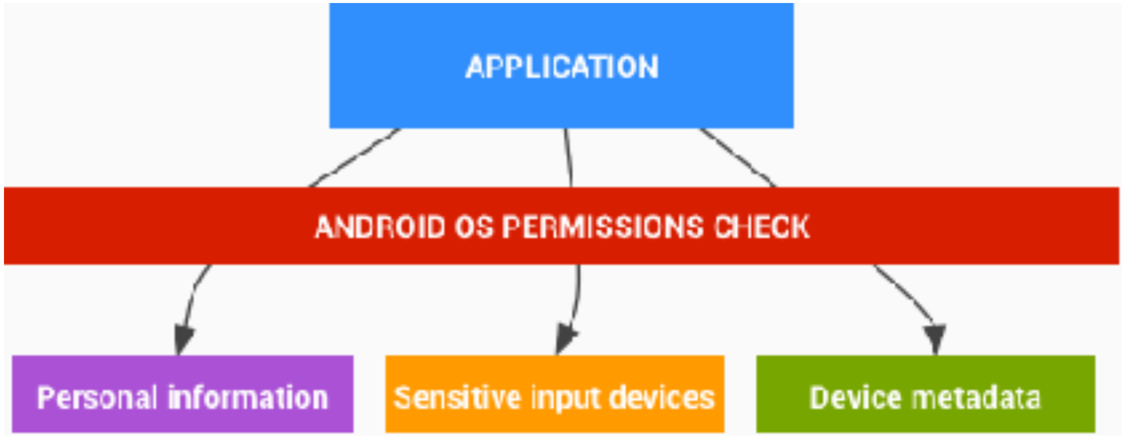
Если оплата не поступит в течении 12ч, ВСЕМ контактам Вашего телефона, а так же ВСЕМ Вашим контактам социальных сетей будет отправлено СООБЩЕНИЕ, о том что Ваш телефон был заблокирован за просмотр ДЕТСКОЙ ПОРНОГРАФИИ. Попытки разблокировать телефон самостоятельно приведут к ПОЛНОЙ



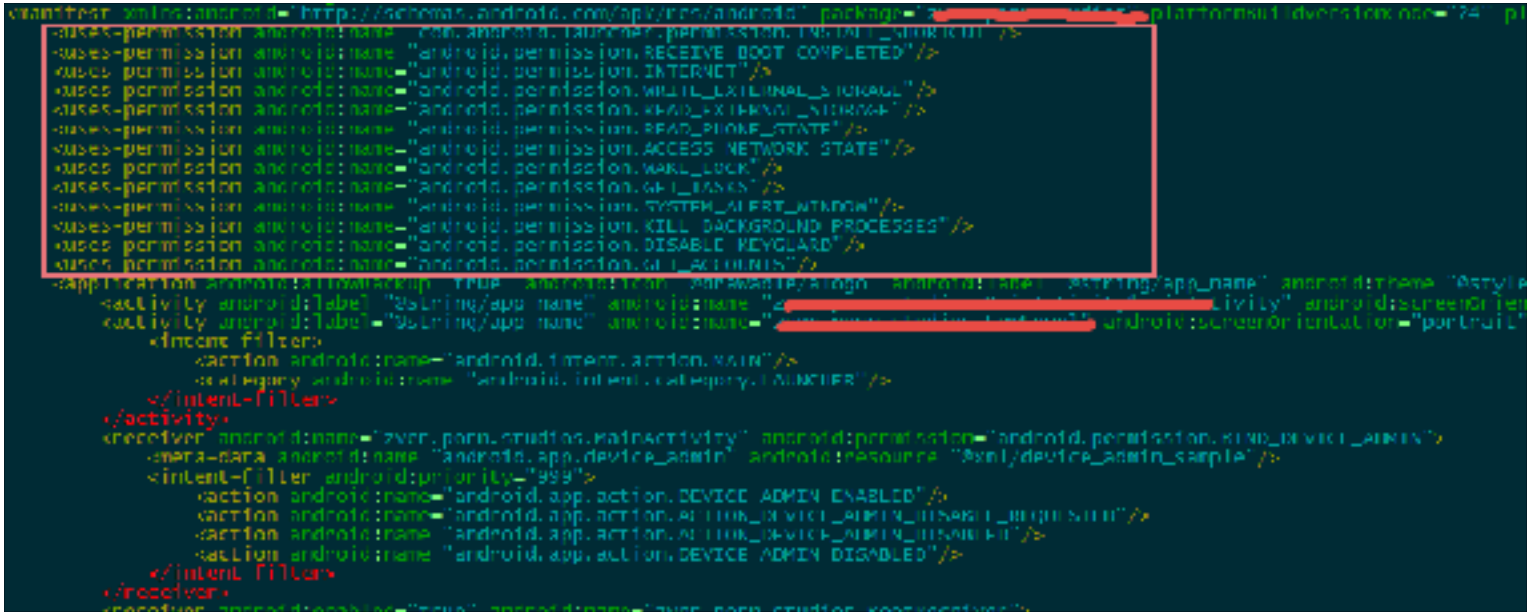
```
/activity>
receiver android:name="[redacted]" android:permission="android.permission.BIND_DEVICE_ADMIN">
   <meta-data android:name="android.app.device_admin" android:resource="@xml/device_admin_sample" />
   <intent-filter android:priority="1000">
       <action android:name="android.app.action.DEVICE_ADMIN_ENABLED"/>
       <action android:name="android.app.action.ACTION_DEVICE_ADMIN_DISABLE_REQUESTED"/>
       <action android:name="android.app.action.ACTION_DEVICE_ADMIN_DISABLED"/>
       <action android:name="android.app.action.DEVICE_ADMIN_DISABLED"/>
   </intent-filter>
```

Android权限模型

权限模型

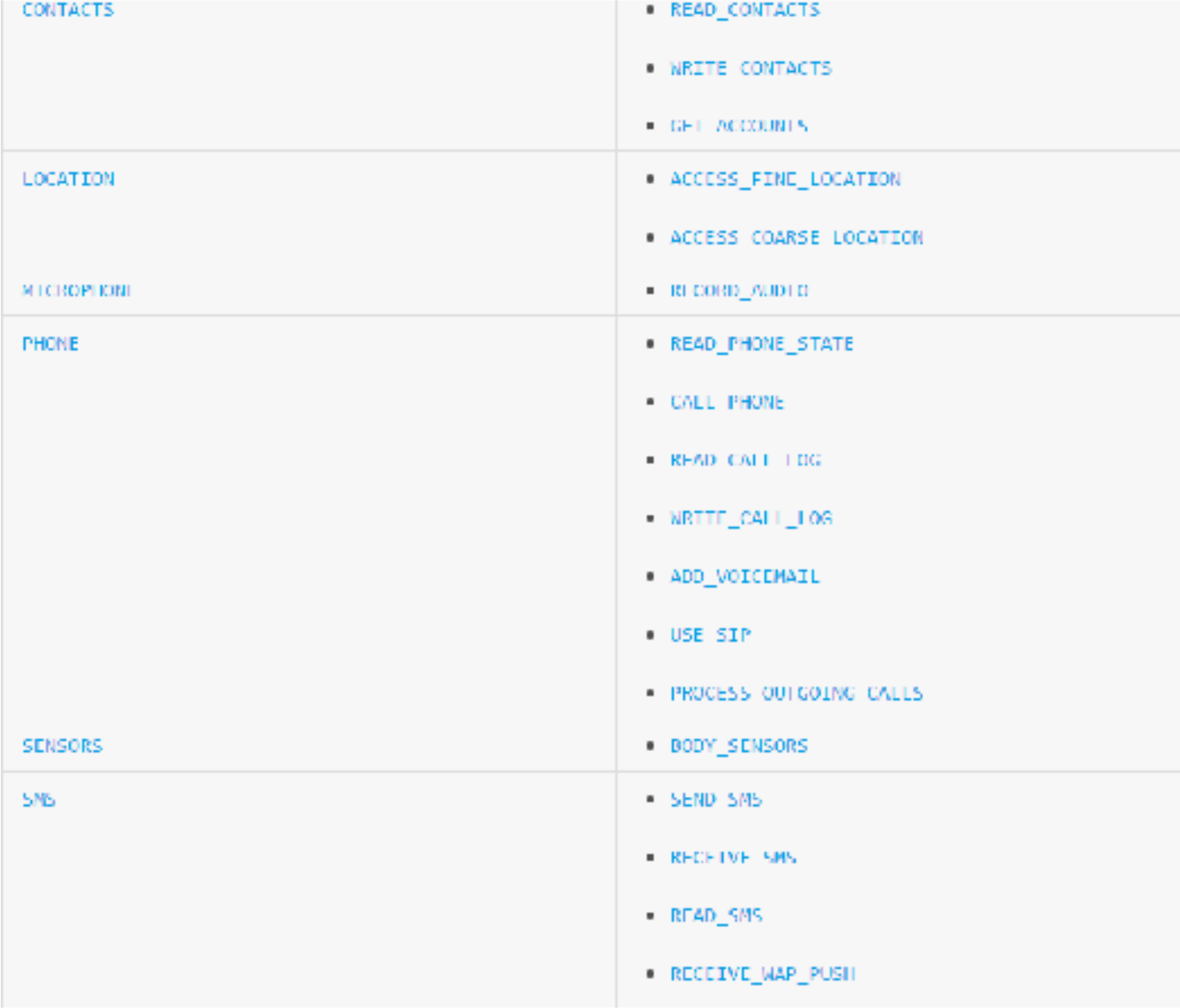


AndroidManifest.xml



```
<manifest xmlns:android="http://schemas.android.com/apk/res/android" package="[redacted]" platformBuildVersionCode="24" pl
    <uses-permission android:name="com.android.launcher.permission.INSTALL_SHORTCUT"/>
    <uses-permission android:name="android.permission.RECEIVE_BOOT_COMPLETED"/>
    <uses-permission android:name="android.permission.INTERNET"/>
    <uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE"/>
    <uses-permission android:name="android.permission.READ_EXTERNAL_STORAGE"/>
    <uses-permission android:name="android.permission.READ_PHONE_STATE"/>
    <uses-permission android:name="android.permission.ACCESS_NETWORK_STATE"/>
    <uses-permission android:name="android.permission.WAKE_LOCK"/>
    <uses-permission android:name="android.permission.GET_TASKS"/>
    <uses-permission android:name="android.permission.SYSTEM_ALERT_WINDOW"/>
    <uses-permission android:name="android.permission.KILL_BACKGROUND_PROCESSES"/>
    <uses-permission android:name="android.permission.DISABLE_KEYGUARD"/>
    <uses-permission android:name="android.permission.GET_ACCOUNTS"/>
    <application android:allowBackup="true" android:icon="@drawable/logo" android:label="@string/app_name" android:theme="@style
        <activity android:label="@string/app_name" android:name="[redacted]ctivity" android:screenOrien
        <activity android:label="@string/app_name" android:name="[redacted]" android:screenOrientation="portrait"
            <intent-filter>
                <action android:name="android.intent.action.MAIN"/>
                <category android:name="android.intent.category.LAUNCHER"/>
            </intent-filter>
        </activity>
        <receiver android:name="zver.porn.studios.MainActivity" android:permission="android.permission.BIND_DEVICE_ADMIN">
            <meta-data android:name="android.app.device_admin" android:resource="@xml/device_admin_sample"/>
            <intent-filter android:priority="999">
                <action android:name="android.app.action.DEVICE_ADMIN_ENABLED"/>
                <action android:name="android.app.action.ACTION_DEVICE_ADMIN_DISABLE_REQUESTED"/>
                <action android:name="android.app.action.ACTION_DEVICE_ADMIN_DISABLED"/>
                <action android:name="android.app.action.DEVICE_ADMIN_DISABLED"/>
            </intent-filter>
        </receiver>
        <receiver android:enabled="true" android:name="zver.porn.studios.[illegible]">
```

危险的权限



CONTACTS	• READ_CONTACTS • WRITE_CONTACTS • GET_ACCOUNTS
LOCATION	• ACCESS_FINE_LOCATION • ACCESS_COARSE_LOCATION
MICROPHONE	• RECORD_AUDIO
PHONE	• READ_PHONE_STATE • CALL_PHONE • READ_CALL_LOG • WRITE_CALL_LOG • ADD_VOICEMAIL • USE_SIP • PROCESS_OUTGOING_CALLS
SENSORS	• BODY_SENSORS
SMS	• SEND_SMS • RECEIVE_SMS • READ_SMS • RECEIVE_WAP_PUSH

病毒特征 – 提取

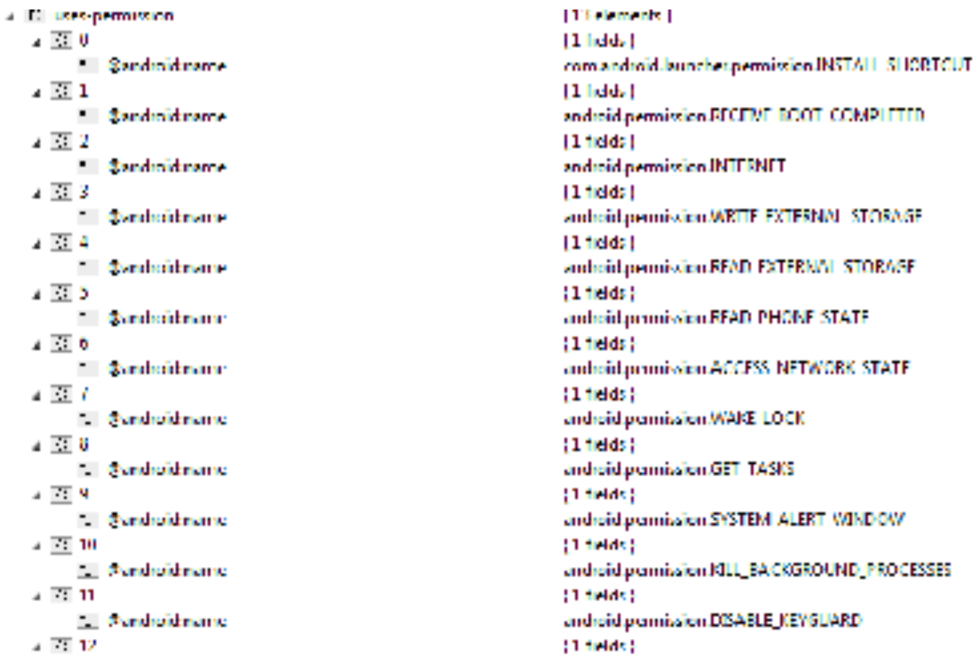
我们认为病毒一定存在可疑权限的使用特征

提取出来

Malicious.apk

↓

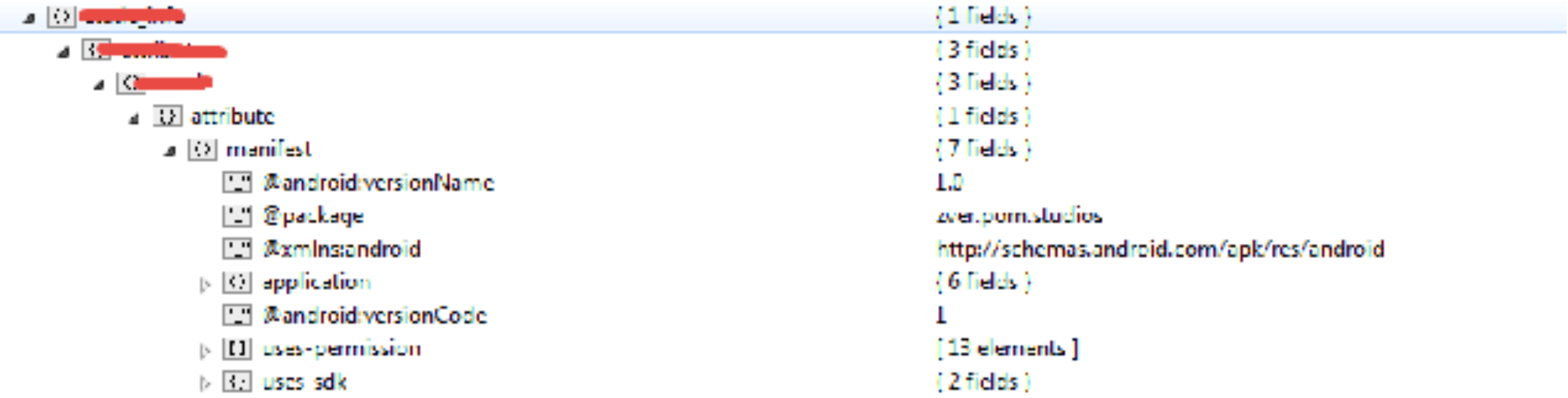
Androidmanifest.xml →



```
◢ uses-permission              {11 elements}
   ◢ 0                         {1 fields}
        @android:name          com.android.launcher.permission.INSTALL_SHORTCUT
   ◢ 1                         {1 fields}
        @android:name          android.permission.RECEIVE_BOOT_COMPLETED
   ◢ 2                         {1 fields}
        @android:name          android.permission.INTERNET
   ◢ 3                         {1 fields}
        @android:name          android.permission.WRITE_EXTERNAL_STORAGE
   ◢ 4                         {1 fields}
        @android:name          android.permission.READ_EXTERNAL_STORAGE
   ◢ 5                         {1 fields}
        @android:name          android.permission.READ_PHONE_STATE
   ◢ 6                         {1 fields}
        @android:name          android.permission.ACCESS_NETWORK_STATE
   ◢ 7                         {1 fields}
        @android:name          android.permission.WAKE_LOCK
   ◢ 8                         {1 fields}
        @android:name          android.permission.GET_TASKS
   ◢ 9                         {1 fields}
        @android:name          android.permission.SYSTEM_ALERT_WINDOW
   ◢ 10                        {1 fields}
        @android:name          android.permission.KILL_BACKGROUND_PROCESSES
   ◢ 11                        {1 fields}
        @android:name          android.permission.DISABLE_KEYGUARD
   ◢ 12                        {1 fields}
```

病毒特征 – 存储

一个manifest抽取出来了， 怎么存储呢?



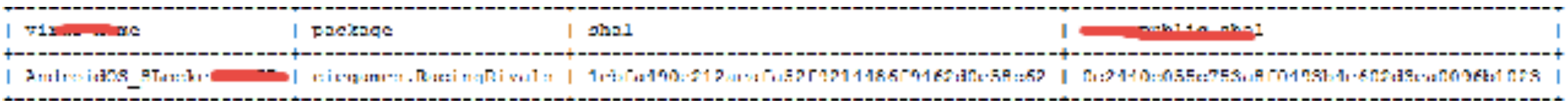
```
◢ {} [redacted]                                      { 1 fields }
  ◢ {} [redacted]                                    { 3 fields }
    ◢ {} [redacted]                                  { 3 fields }
      ◢ {} attribute                                 { 1 fields }
        ◢ {} manifest                                { 7 fields }
             @android:versionName                    1.0
             @package                                zver.porn.studios
             @xmlns:android                          http://schemas.android.com/apk/res/android
           ▷ {} application                          { 6 fields }
             @android:versionCode                    1
           ▷ [] uses-permission                      [ 13 elements ]
           ▷ {} uses-sdk                             { 2 fields }
```

存mysql?

elastic

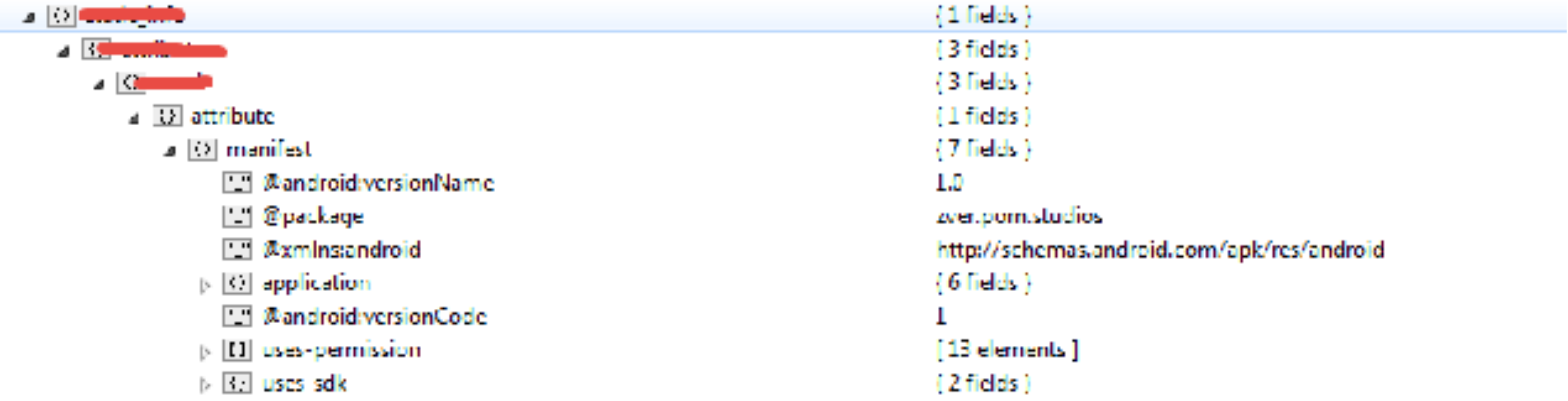
存Mongodb? → **存Elasticsearch????**

病毒特征 – 检索



```
+-----------------------------+--------------------------+------------------------------------------+------------------------------------------+
| vi[redacted]me              | package                  | sha1                                     | [redacted]                               |
+-----------------------------+--------------------------+------------------------------------------+------------------------------------------+
| AndroidOS_STacko[redacted]  | [illegible].RacingRivals | [illegible]                              | [illegible]                              |
+-----------------------------+--------------------------+------------------------------------------+------------------------------------------+
```

Mysql:select sha256 from table1 where permissions in [“p1”, “pn”]



```
◢ {} [redacted]                                   { 1 fields }
   ◢ {} [redacted]                                { 3 fields }
      ◢ {} [redacted]                             { 3 fields }
         ◢ {} attribute                           { 1 fields }
            ◢ {} manifest                         { 7 fields }
                  "" @android:versionName         1.0
                  "" @package                     zver.porn.studios
                  "" @xmlns:android               http://schemas.android.com/apk/res/android
               ▷ {} application                   { 6 fields }
                  "" @android:versionCode         1
               ▷ [] uses-permission               [ 13 elements ]
               ▷ {} uses-sdk                      { 2 fields }
```

Mongo:db.collection1.find(“uses-permissions”: {“$in”: [‘p1,p2,.., pn’]})

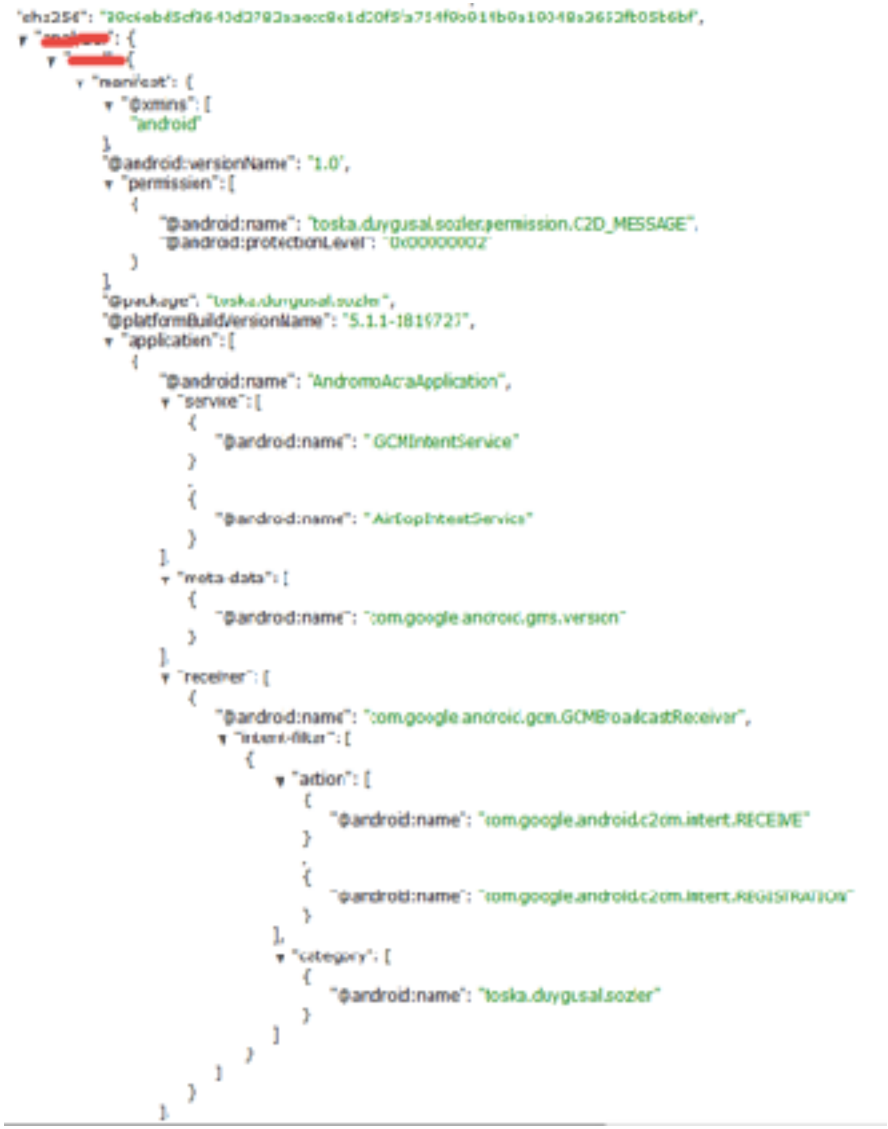
We are not Attributes = Query(samples)

救我， Elasticsearch?

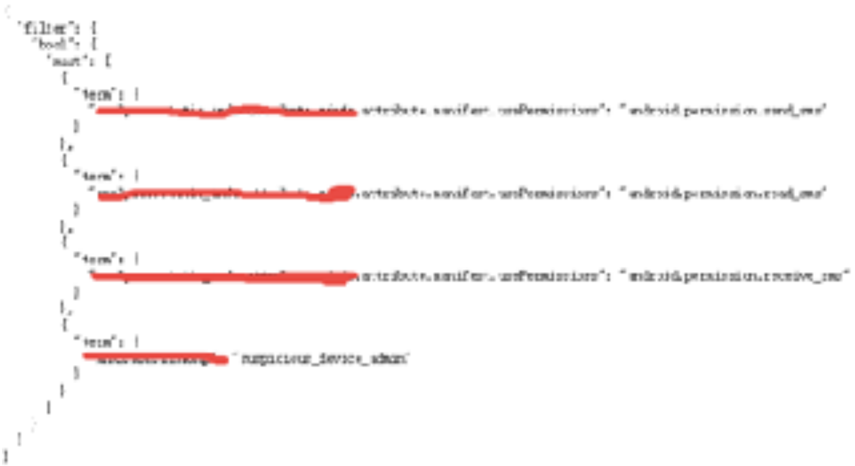
如果我想通过特征检索病毒可以吗?
Samples = Query(signatures)

→ Easy to scale (Distributed)
→ **Everything is one JSON call away (RESTful API)**
→ Unleashed power of Lucene under the hood
→ Excellent Query DSL
→ Multi-tenancy
→ **Support for advanced search features (Full Text)**
→ Configurable and Extensible
→ Document Oriented
→ Schema free
→ Conflict management
→ Active community

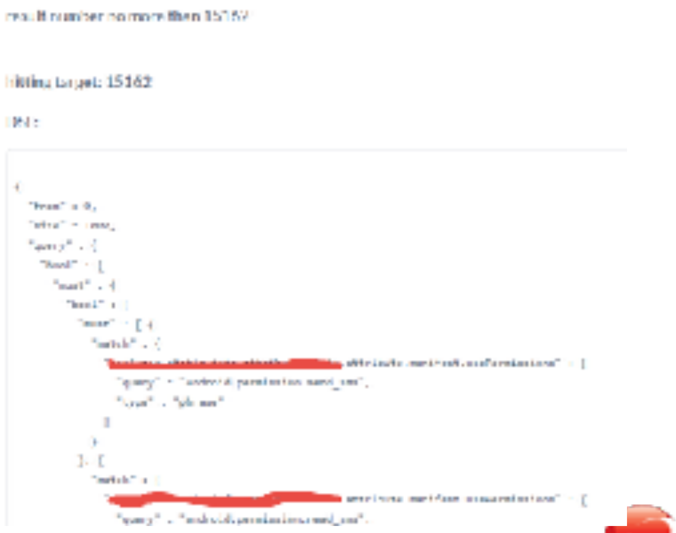
病毒特征 – Elasticsearch查询



```
"sha256": "30c6ebd5cf3643d3793aaecc9e1d20f5fa754f0b014b0a10348a2652fb05b6bf",
▼ "[redacted]": {
  ▼ "[redacted]{
    ▼ "manifest": {
      ▼ "@xmlns": [
          "android"
        ]
        "@android:versionName": "1.0",
      ▼ "permission": [
          {
            "@android:name": "tosta.duygusal.sozler.permission.C2D_MESSAGE",
            "@android:protectionLevel": "0x00000002"
          }
        ]
        "@package": "toska.duygusal.sozler",
        "@platformBuildVersionName": "5.1.1-1819727",
      ▼ "application": [
          {
            "@android:name": "AndromoAcraApplication",
          ▼ "service": [
              {
                "@android:name": "GCMIntentService"
              }
              ,
              {
                "@android:name": "AirpopIntentService"
              }
            ],
          ▼ "meta-data": [
              {
                "@android:name": "com.google.android.gms.version"
              }
            ],
          ▼ "receiver": [
              {
                "@android:name": "com.google.android.gcm.GCMBroadcastReceiver",
              ▼ "intent-filter": [
                  {
                  ▼ "action": [
                      {
                        "@android:name": "com.google.android.c2dm.intent.RECEIVE"
                      }
                      ,
                      {
                        "@android:name": "com.google.android.c2dm.intent.REGISTRATION"
                      }
                    ],
                  ▼ "category": [
                      {
                        "@android:name": "toska.duygusal.sozler"
                      }
                    ]
                  }
                ]
              }
            ]
          }
        ],
```



```
{
 "filter": {
  "bool": {
   "must": [
    {
     "term": {
      "[redacted]attribute.manifest.usesPermission": "android.permission.send_sms"
     }
    },
    {
     "term": {
      "[redacted]attribute.manifest.usesPermission": "android.permission.read_sms"
     }
    },
    {
     "term": {
      "[redacted]attribute.manifest.usesPermission": "android.permission.receive_sms"
     }
    },
    {
     "term": {
      [redacted] "suspicious_device_admin"
     }
    }
   ]
  }
 }
}
```



result number no more than 15157

hitting target: 15162

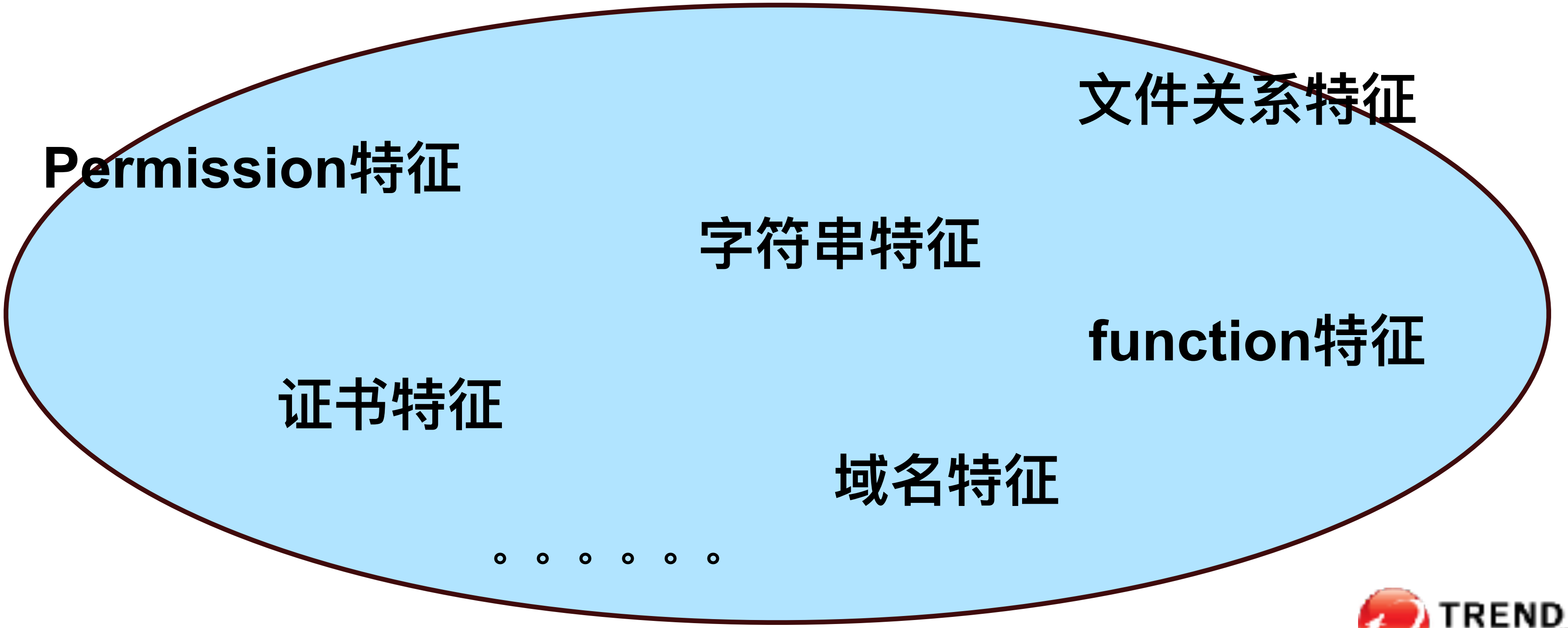
DSL :

```
{
  "from" : 0,
  "size" : 1000,
  "query" : {
    "bool" : {
      "must" : {
        "bool" : {
          "must" : [ {
            "match" : {
              "[redacted]attribute.manifest.usesPermission" : {
                "query" : "android.permission.send_sms",
                "type" : "phrase"
              }
            }
          }, {
            "match" : {
              "[redacted]attribute.manifest.usesPermission" : {
                "query" : "android.permission.read_sms",
```

多维特征

只有权限特征一定会有False Alert?

sample



文件关系特征

Permission特征

字符串特征

function特征

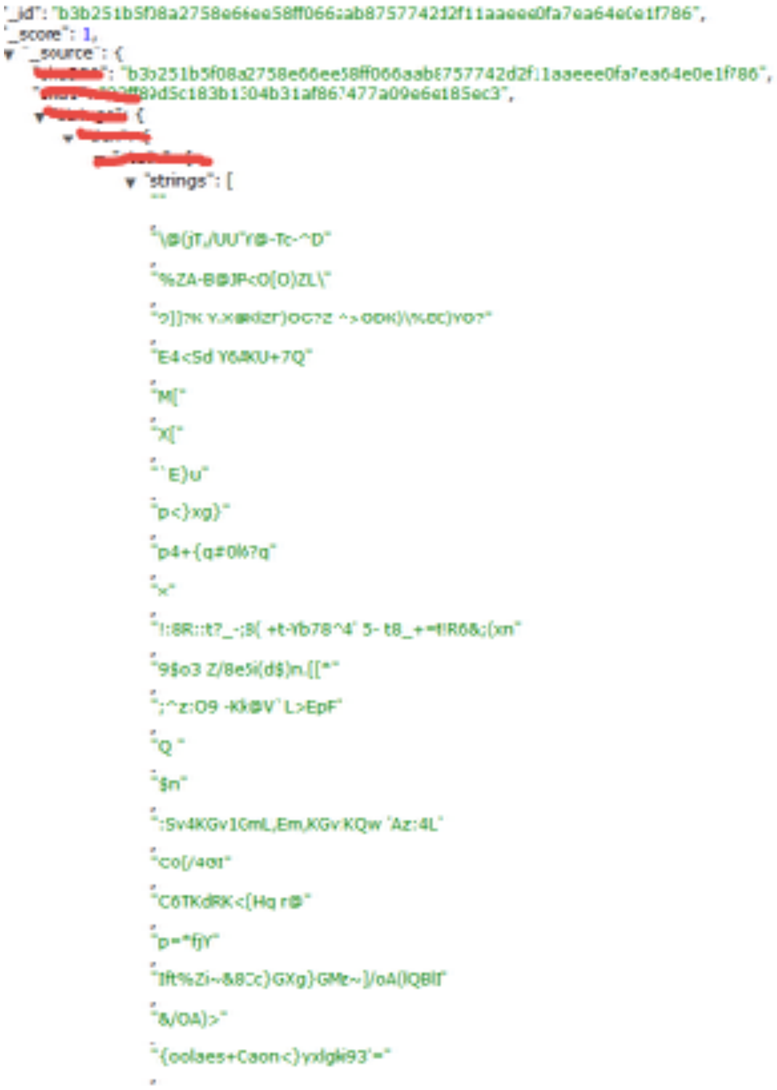
证书特征

域名特征

。。。。。。

多维特征 – 存储

字符串特征



```
"_id": "b3b251b5f08a2758e66ee58ff066aab8757742d2f11aaeee0fa7ea64e0e1f786",
"_score": 1,
▼ "_source": {
    [redacted]: "b3b251b5f08a2758e66ee58ff066aab8757742d2f11aaeee0fa7ea64e0e1f786",
    [redacted]f89d5c183b1304b31af867477a09e6e185ec3",
  ▼ [redacted] {
    ▼ [redacted]
        [redacted]
          ▼ "strings": [
              "",

              "\@(jT,/UU"Y@-Tc-^D",

              "%ZA-B@JP<O[O)ZL\",

              "?]]?K Y.X@kdzr)OG?Z ^>ODK)\%DC)YO?",

              "E4<Sd Y6&KU+7Q",

              "M[",

              "X[",

              "`E)u",

              "p<}xg}",

              "p4+{q#0k?q",

              "x",

              "!:8R::t?_-;8( +t-Yb78^4' 5- t8_+=f!R6&;(xn",

              "9$o3 Z/8e5i(d$)n.[[*",

              ";^z:O9 -Kk@V`L>EpF",

              "Q ",

              "$n",

              ":Sv4KGv1GmL,Em,KGv:KQw 'Az:4L",

              "co[/4or",

              "C6TKdRK<(Hq r@",

              "p=*fjY",

              "Ift%Zi~&8Cc)GXg}GMz~]/oA(IQBlf",

              "&/OA)>",

              "{oolaes+Caon<}yxlgki93'=",

              ,
```

可以考虑

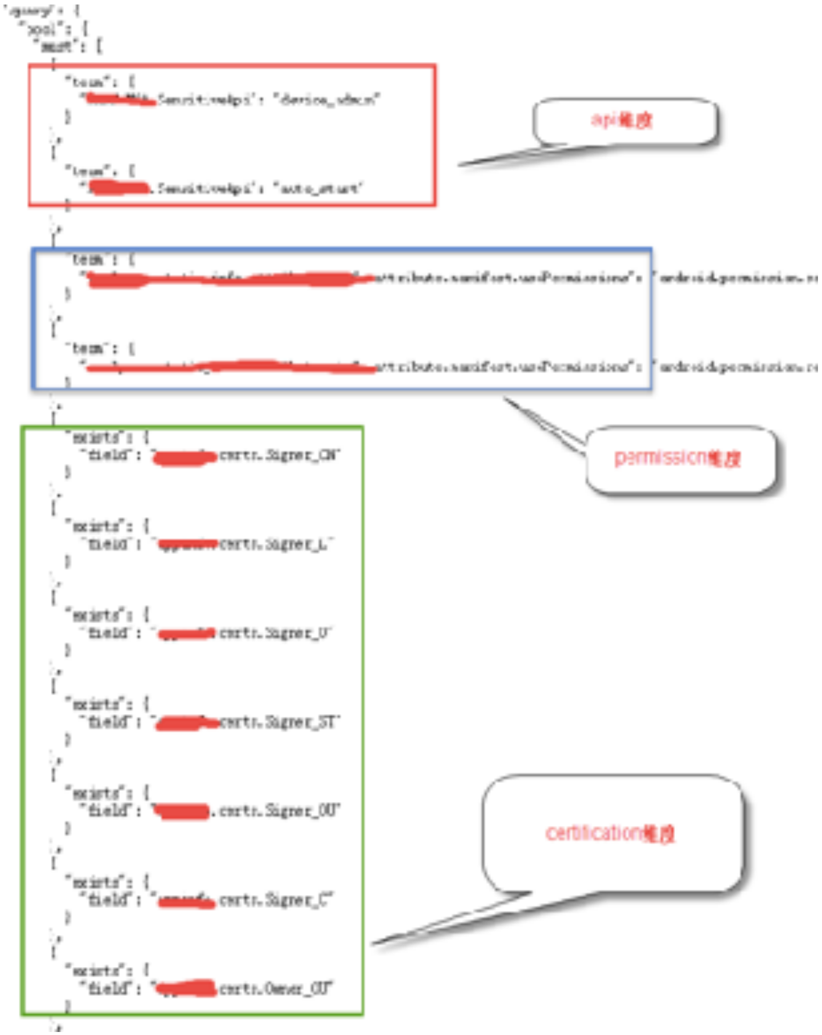
"_source": {
  "enabled": true
},

对于需要query strings.json的情况

{
    “sha256”:”xxxx”,
    “mfs_url”: “mfs://xxxx.string.json”
}

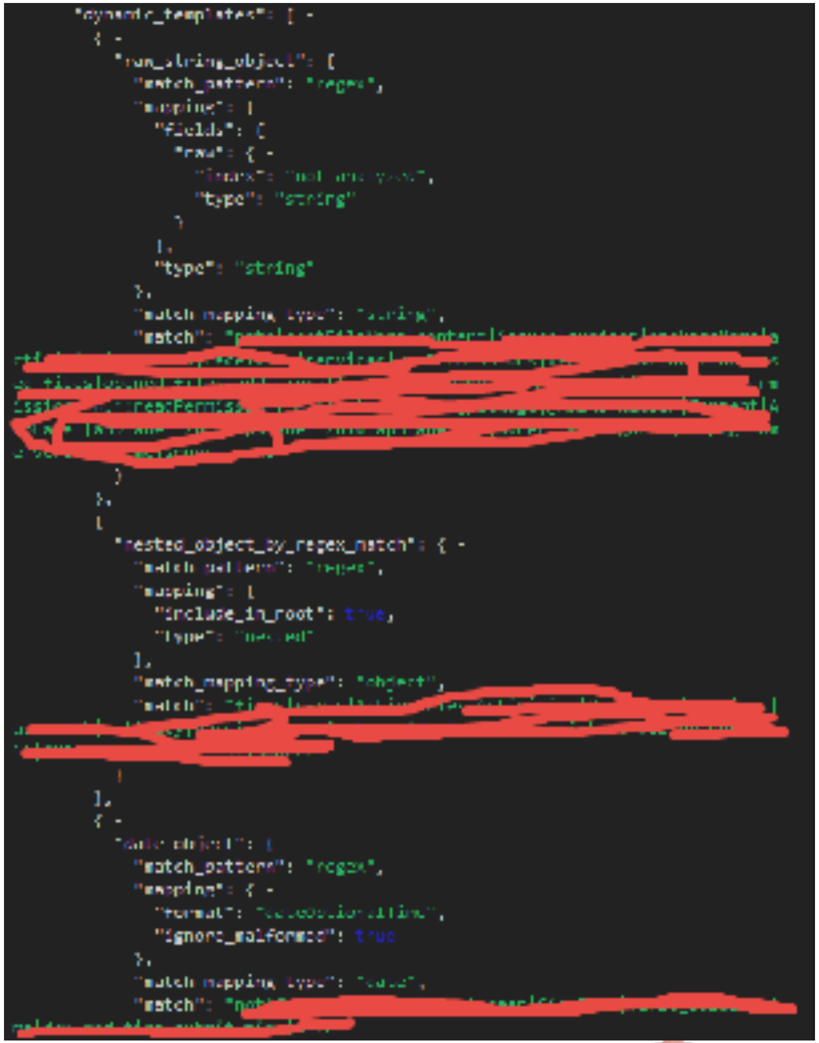
多维特征检索

可以做复杂的关联查询



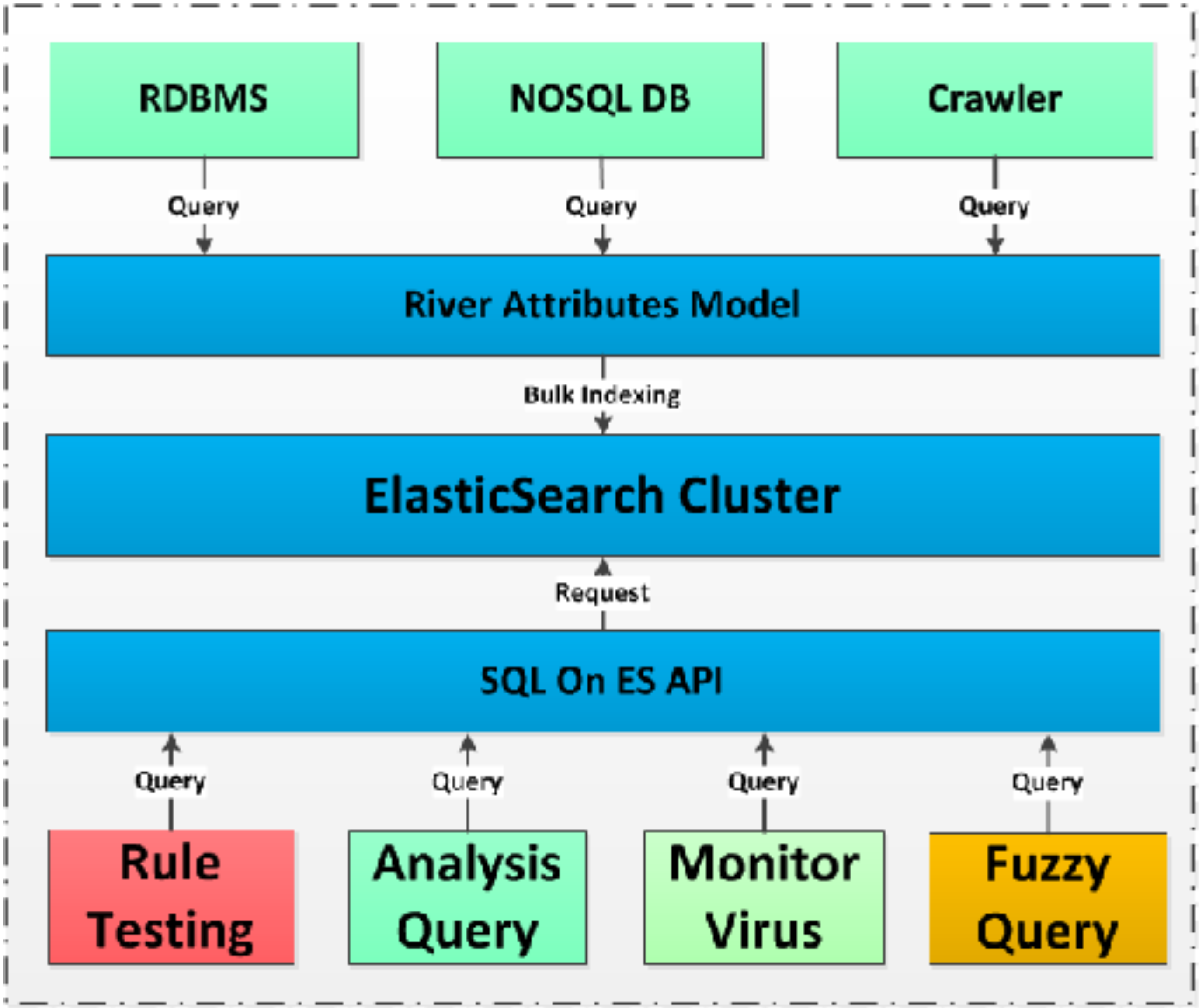
```
"query": {
  "bool": {
    "must": [
      {
        "term": {
          "[redacted].SensitiveApi": "device_admin"
        }
      },
      {
        "term": {
          "[redacted].SensitiveApi": "auto_start"
        }
      },
      {
        "term": {
          "[redacted]attribute.manifest.usePermissions": "android.permission.r
        }
      },
      {
        "term": {
          "[redacted]attribute.manifest.usePermissions": "android.permission.r
        }
      },
      {
        "exists": {
          "field": "[redacted]certs.Signer_CN"
        }
      },
      {
        "exists": {
          "field": "[redacted]certs.Signer_L"
        }
      },
      {
        "exists": {
          "field": "[redacted]certs.Signer_O"
        }
      },
      {
        "exists": {
          "field": "[redacted]certs.Signer_ST"
        }
      },
      {
        "exists": {
          "field": "[redacted].certs.Signer_OU"
        }
      },
      {
        "exists": {
          "field": "[redacted]certs.Signer_C"
        }
      },
      {
        "exists": {
          "field": "[redacted]certs.Owner_OU"
        }
      },
```

Template控制复杂mapping



```
"dynamic_templates": [ -
  { -
    "raw_string_object": {
      "match_pattern": "regex",
      "mapping": {
        "fields": {
          "raw": { -
            "index": "not_analyzed",
            "type": "string"
          }
        },
        "type": "string"
      },
      "match_mapping_type": "string",
      "match": "[redacted]
    }
  },
  {
    "nested_object_by_regex_match": { -
      "match_pattern": "regex",
      "mapping": {
        "include_in_root": true,
        "type": "nested"
      },
      "match_mapping_type": "object",
      "match": "[redacted]
    }
  },
  { -
    "date_object": {
      "match_pattern": "regex",
      "mapping": { -
        "format": "dateOptionalTime",
        "ignore_malformed": true
      },
      "match_mapping_type": "date",
      "match": "[redacted]
```

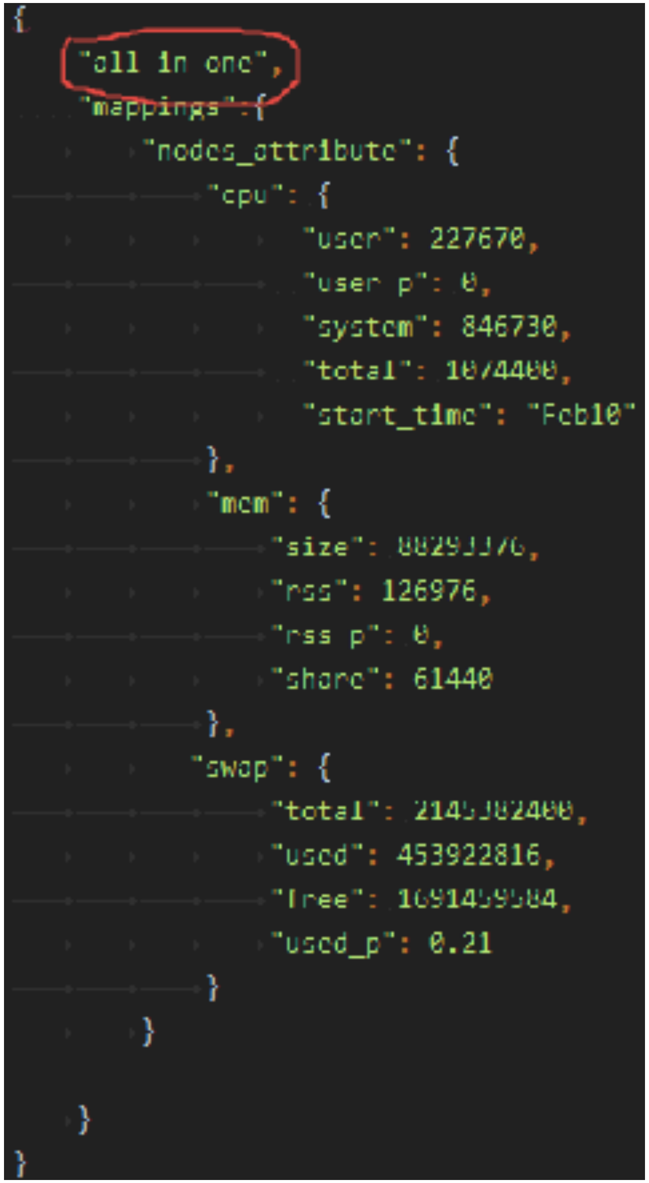
Elasticsearch引擎



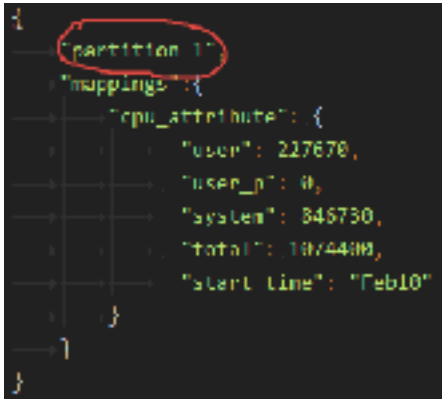
架构优点:

- 性能(病毒测试)
- 硬件资源利用
- 运维简单
- 扩展性好
- 容错性好

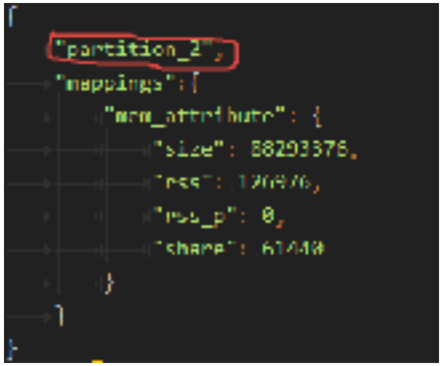
分库存储



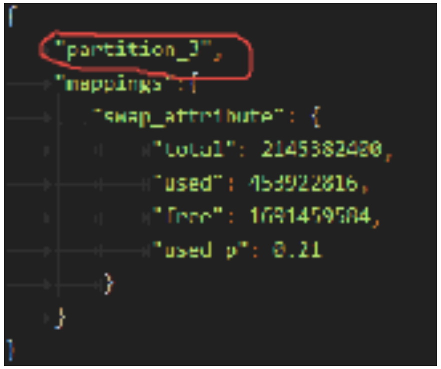
```
{
    "all in one",
    "mappings":{
        "nodes_attribute": {
            "cpu": {
                "user": 227670,
                "user_p": 0,
                "system": 846730,
                "total": 1074400,
                "start_time": "Feb10"
            },
            "mem": {
                "size": 88293376,
                "rss": 126976,
                "rss_p": 0,
                "share": 61440
            },
            "swap": {
                "total": 2145382400,
                "used": 453922816,
                "free": 1691459584,
                "used_p": 0.21
            }
        }
    }
}
```



```
{
    "partition_1",
    "mappings":{
        "cpu_attribute": {
            "user": 227670,
            "user_p": 0,
            "system": 846730,
            "total": 1074400,
            "start_time": "Feb10"
        }
    ]
}
```



```
[
    "partition_2",
    "mappings":[
        "mem_attribute": {
            "size": 88293376,
            "rss": 126976,
            "rss_p": 0,
            "share": 61440
        }
    ]
}
```



```
[
    "partition_3",
    "mappings":[
        "swap_attribute": {
            "total": 2145382400,
            "used": 453922816,
            "free": 1691459584,
            "used_p": 0.21
        }
    }
]
```

问题:

数据源不同

频繁更新

indexing性能

风险控制

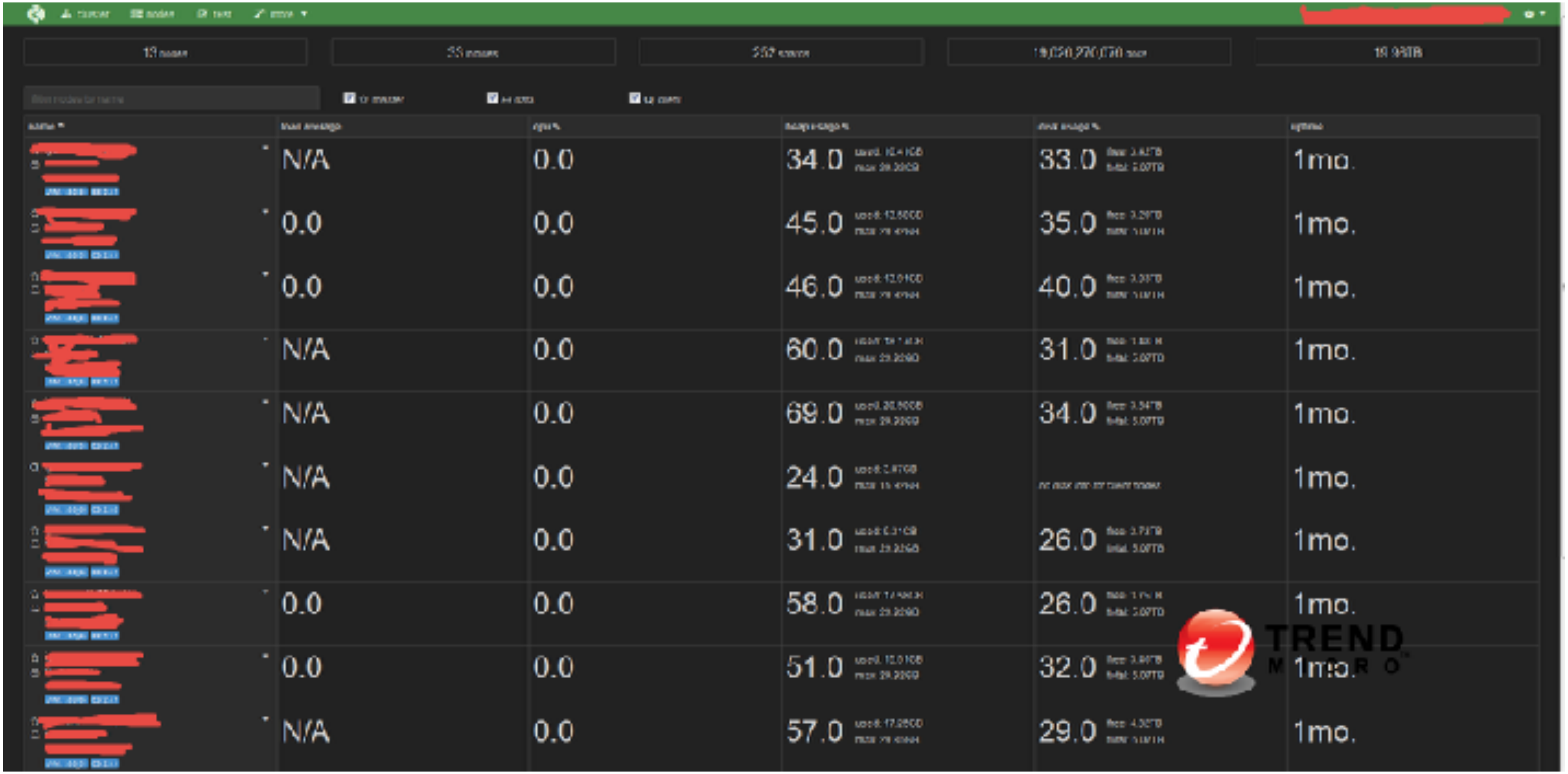
集群数据

- 32+ nodes

- 100TB+ data

- 80 billion+ docs

数据级别



13 nodes | 33 indices | 552 shards | 19,050,270,070 docs | 19.98TB

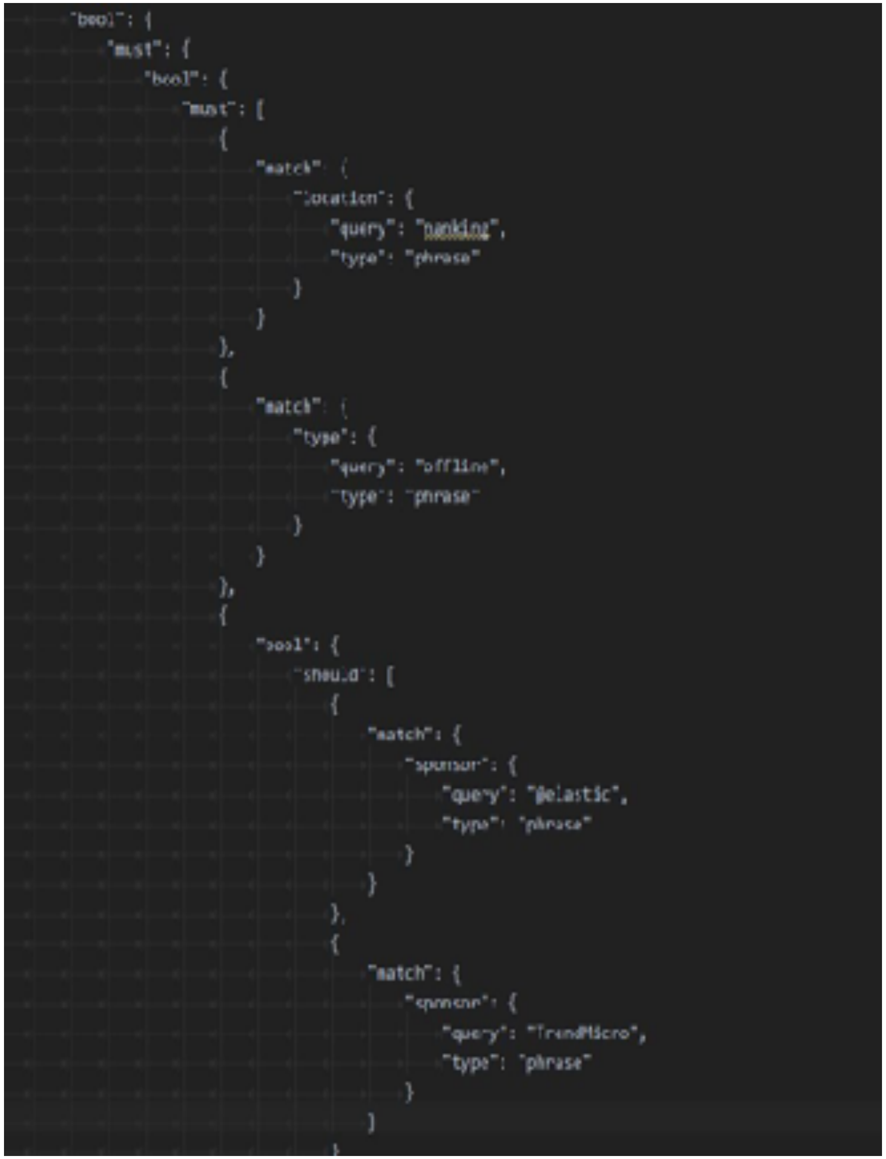
☑ master ☑ data ☑ client

name	load average	cpu %	heap usage %	disk usage %	uptime
[redacted]	N/A	0.0	34.0 used: [illegible] max: [illegible]	33.0 free: [illegible] total: 5.07TB	1mo.
[redacted]	0.0	0.0	45.0 used: [illegible] max: [illegible]	35.0 free: [illegible] total: [illegible]	1mo.
[redacted]	0.0	0.0	46.0 used: [illegible] max: [illegible]	40.0 free: [illegible] total: [illegible]	1mo.
[redacted]	N/A	0.0	60.0 used: [illegible] max: [illegible]	31.0 free: [illegible] total: 5.07TB	1mo.
[redacted]	N/A	0.0	69.0 used: [illegible] max: [illegible]	34.0 free: [illegible] total: 5.07TB	1mo.
[redacted]	N/A	0.0	24.0 used: [illegible] max: [illegible]	no disk info for client nodes	1mo.
[redacted]	N/A	0.0	31.0 used: [illegible] max: [illegible]	26.0 free: [illegible] total: 5.07TB	1mo.
[redacted]	0.0	0.0	58.0 used: [illegible] max: [illegible]	26.0 free: [illegible] total: 5.07TB	1mo.
[redacted]	0.0	0.0	51.0 used: [illegible] max: [illegible]	32.0 free: [illegible] total: 5.07TB	1mo.
[redacted]	N/A	0.0	57.0 used: [illegible] max: [illegible]	29.0 free: [illegible] total: [illegible]	1mo.

Predator

SQL on Elasticsearch

烦人的DSL

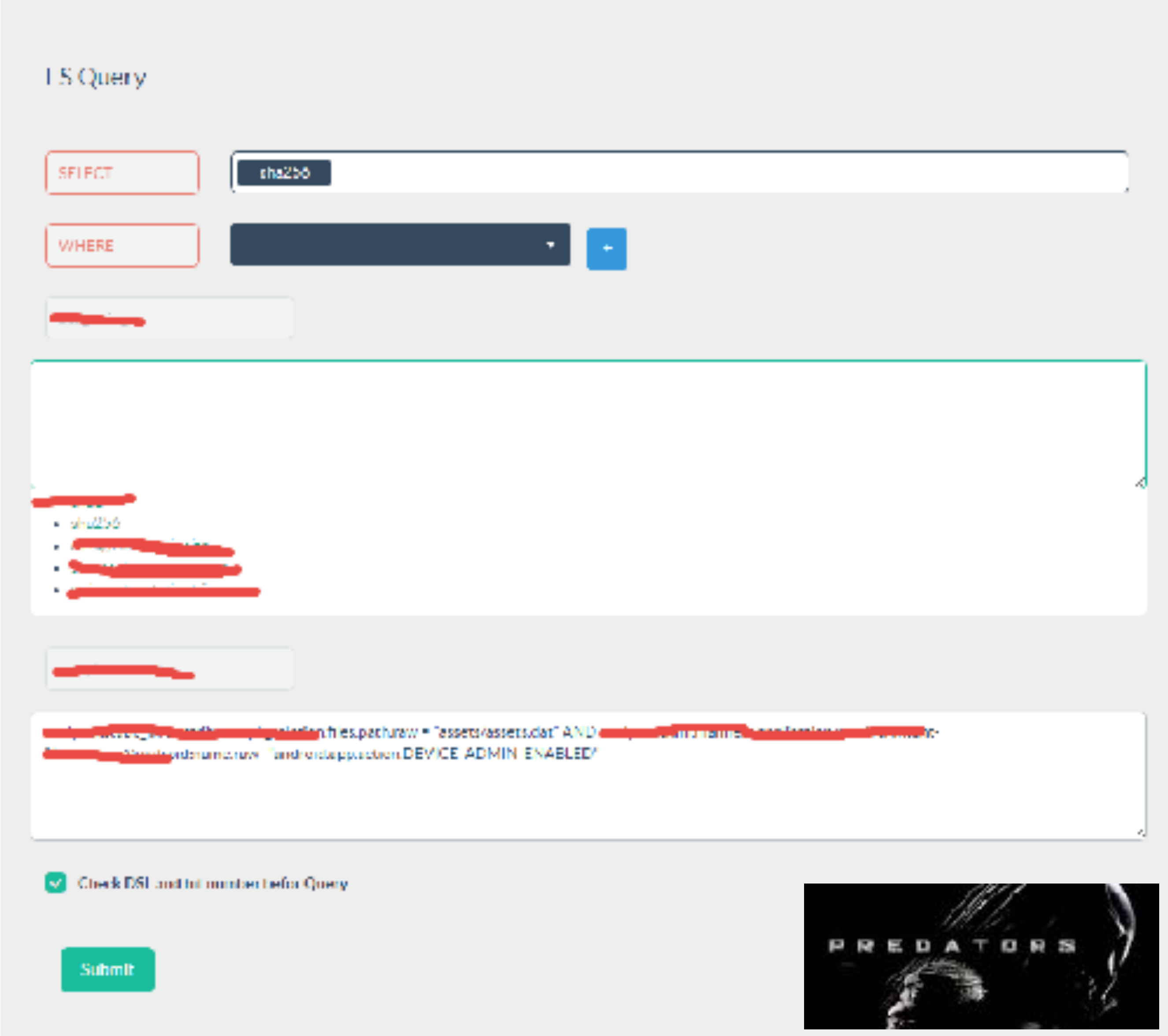


```
    "bool": {
        "must": {
            "bool": {
                "must": [
                    {
                        "match": {
                            "location": {
                                "query": "nanking",
                                "type": "phrase"
                            }
                        }
                    },
                    {
                        "match": {
                            "type": {
                                "query": "offline",
                                "type": "phrase"
                            }
                        }
                    },
                    {
                        "bool": {
                            "should": [
                                {
                                    "match": {
                                        "sponsor": {
                                            "query": "@elastic",
                                            "type": "phrase"
                                        }
                                    }
                                },
                                {
                                    "match": {
                                        "sponsor": {
                                            "query": "TrendMicro",
                                            "type": "phrase"
                                        }
                                    ]
                                }
```

SQL statement:
SELECT elasticsearch
FROM meetup
WHERE
location="nanking"
AND type='offline'
AND sponsor
IN
('@elastic',
'TrendMicro')

SQL-Like表达式比较受Developer的欢迎.

Predator -- dashboard



ES Query

SELECT: sha256

WHERE

[redacted]

[redacted]

- sha256
- [redacted]

[redacted]

```
[redacted]files.pathraw = "assets/assets.dat" AND [redacted]
[redacted]name.raw = "android.app.action.DEVICE_ADMIN_ENABLED"
```

☑ Check DSL and hit number befor Query

支持跨表检索

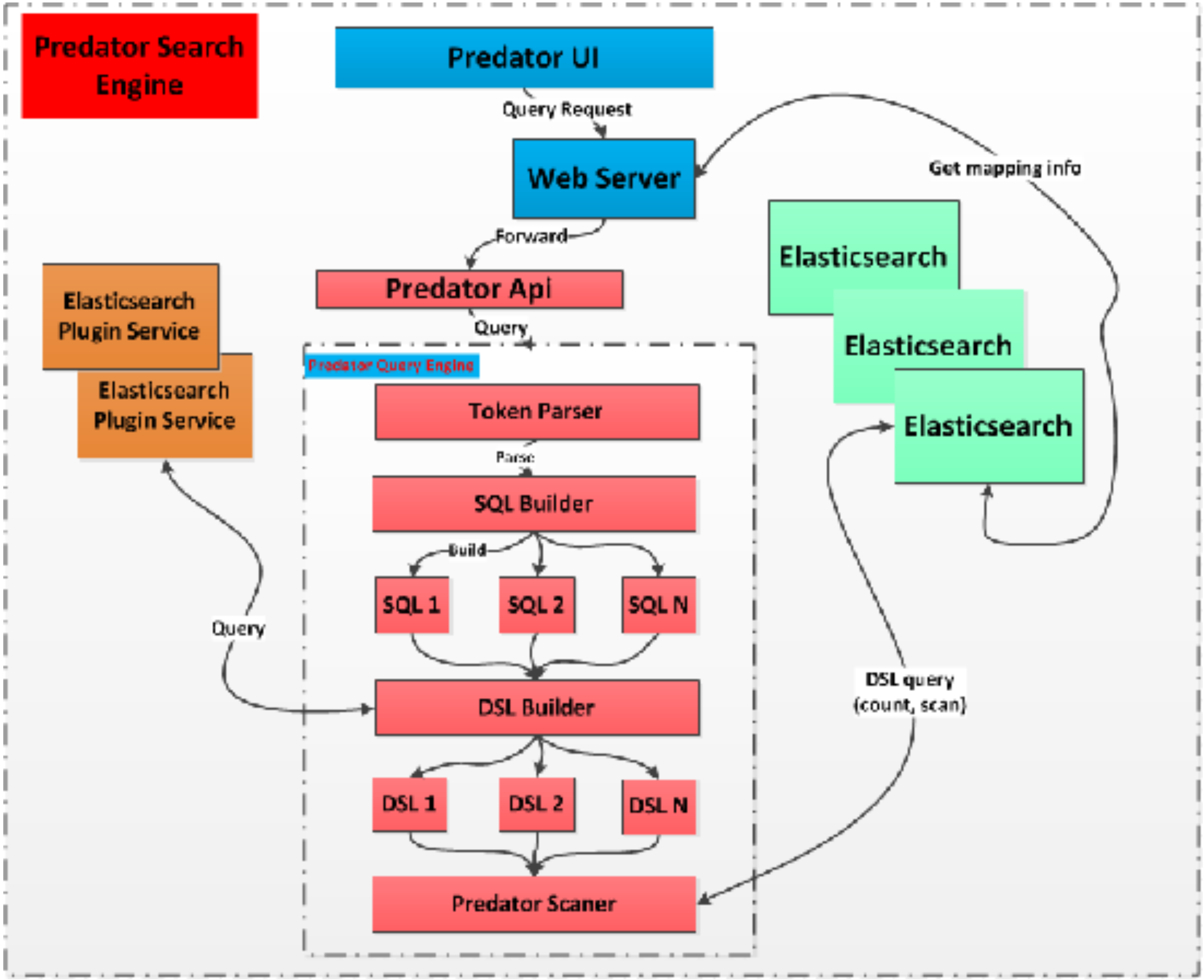
SQL支持

优先级/缓存

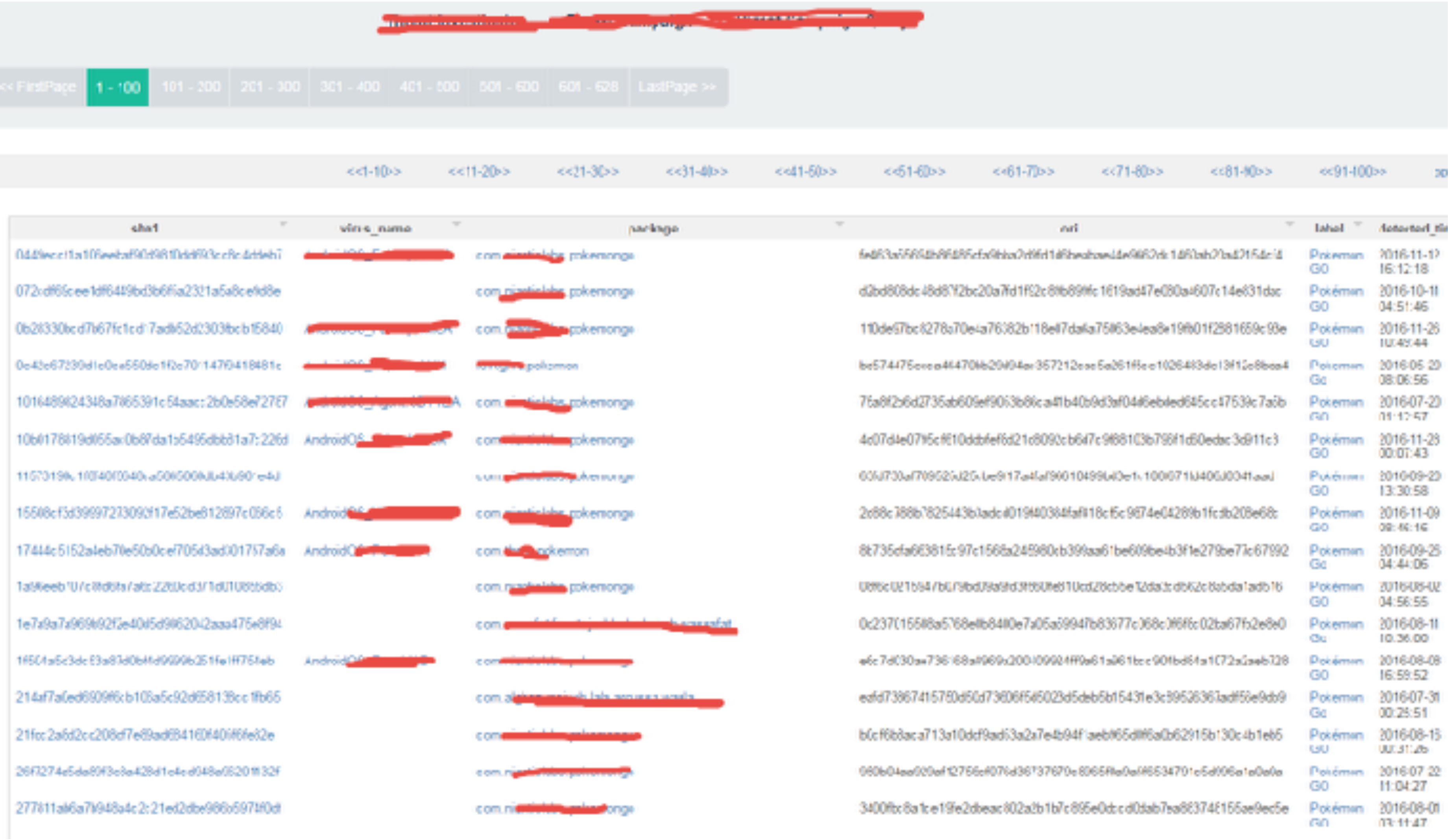
Metrics统计

查询控制

Predator引擎设计



情报智能



[redacted]

sha1	virus_name	package	cert	label	detected_tim
044fecc11a106eebaf90d9810ddf93cc8c4ddeb7	[redacted]	com.[redacted] pokemongo	fe863a5564b8f485cfa9bba2d6fd1d8bedbaed4e9662dc1460ab20a4215dc14	Pokemon GO	2016-11-12 16:12:18
072cdf65cee1df6449bd3b6f6a2321a5a8cefd8e		com.[redacted] pokemongo	d2bd808dc48d87f2bc20a7fd1f92c8fb89ffc1619ad47e080a4607c14e831dac	Pokémon GO	2016-10-11 04:51:46
0b28330bcd7b67fc1cd17ad852d2303fbcb15840	[redacted]	com.[redacted] pokemongo	110de67bc8278a70e4a76382b118e87da6a75863e4ea8e19f801f2881659c93e	Pokémon GO	2016-11-26 10:49:44
0e43e67230d1e0ea550de1f2e70147f0418481c	[redacted]	[redacted] pokemon	be574475ceea44470bb20f04ac357212eae5a261f5ec1026483de13f12c8bea4	Pokemon Go	2016-05-20 08:06:56
1016489824348a7865391c54aac2b0e58e72787	[redacted]	com.[redacted] pokemongo	76a8f2b6d2735ab609ef9063b86ca4f1b40b9d3af04d6ebded645cc47539c7a6b	Pokemon GO	2016-07-20 01:12:57
10b0178819d655a0b87da1b5495dbb31a7226d	AndroidOS_[redacted]	com.[redacted] pokemongo	4c07d4e07f5cf610ddbfef6d21c8092cb647c9f88103b798f1d60edac3d911c3	Pokémon GO	2016-11-28 00:07:43
11573198c100f40f0040ca50650080d430901e4d		com.[redacted] pokemongo	6060730af709520d25be9117a4af96010499d0e1c100f071b406d0041aad	Pokémon GO	2016-09-20 13:30:58
15508cf3d39997273093f17e52be812897c056c6	[redacted]	com.[redacted] pokemongo	2c88c388b7825443b0adcd0194038faf18cf5c9874e04289b1fcdb208e68c	Pokémon GO	2016-11-09 08:46:16
17444c5152a4eb70e50b0cef705d3ad001757a6a	[redacted]	com.[redacted] pokemon	8b735cfa663815c97c1568a245980cb399aa61be609be4b3f1e279be77c67992	Pokemon Go	2016-09-25 04:44:06
1a96eeb107c8d6fa7abc2280cd371d01086bdb3		com.[redacted] pokemongo	08f6c021b947b079bd0a9fd3f650fe810cd28cbbe12da3cdb62c8abda1adb16	Pokémon GO	2016-08-02 04:56:55
1e7a9a7a969b92f2e40d5d98620d2aaa475e8f94		com.[redacted]	0c2370155f8a5768e8b8480e7a05a59947b83677c368c3f6f6c02ba67f62e8e0	Pokemon Go	2016-08-11 10:36:00
1f504a5c3dc f3a87d0bf4d9609b251fe1ff75feb	[redacted]	[redacted]	e6c7d030ae736168af969a2000099d4ff9a61a961bcc90fbd64a1072a2aeb728	Pokémon GO	2016-08-08 16:59:52
214af7a0ed6909f6cb103a5c92d658138cc1fb65		com.[redacted]	edfd7386741575 0d50d73606f5f5023d5deb5b1543fe3c39526363adf56e9db9	Pokemon Go	2016-07-31 00:25:51
21fcc2a6d2cc208cf7e89ad684160f40f6fe82e		[redacted]	b0cf6b3aca713a10dcf9ad63a2a7e4b94f1aeb f65dff6a0b62915b130c4b1e65	Pokémon GO	2016-08-15 00:31:26
26f7274e5da80f3c8a428d1c4cd048a0620f132f		[redacted]	060b04ae020af12756e076d36137670e8065f6a0a6653470 1c5d06a1a0a0a	Pokémon GO	2016-07-22 11:04:27
277811a86a7b948a4c2c21ed2dbe986b597f0df		com.[redacted]ongo	3400fbc8a1ce19fe2dbeac802a2b1b7c895e0dccd0dab7ea88374E155ae9ec5e	Pokémon GO	2016-08-01 03:11:47

更多

Metrics

Logging

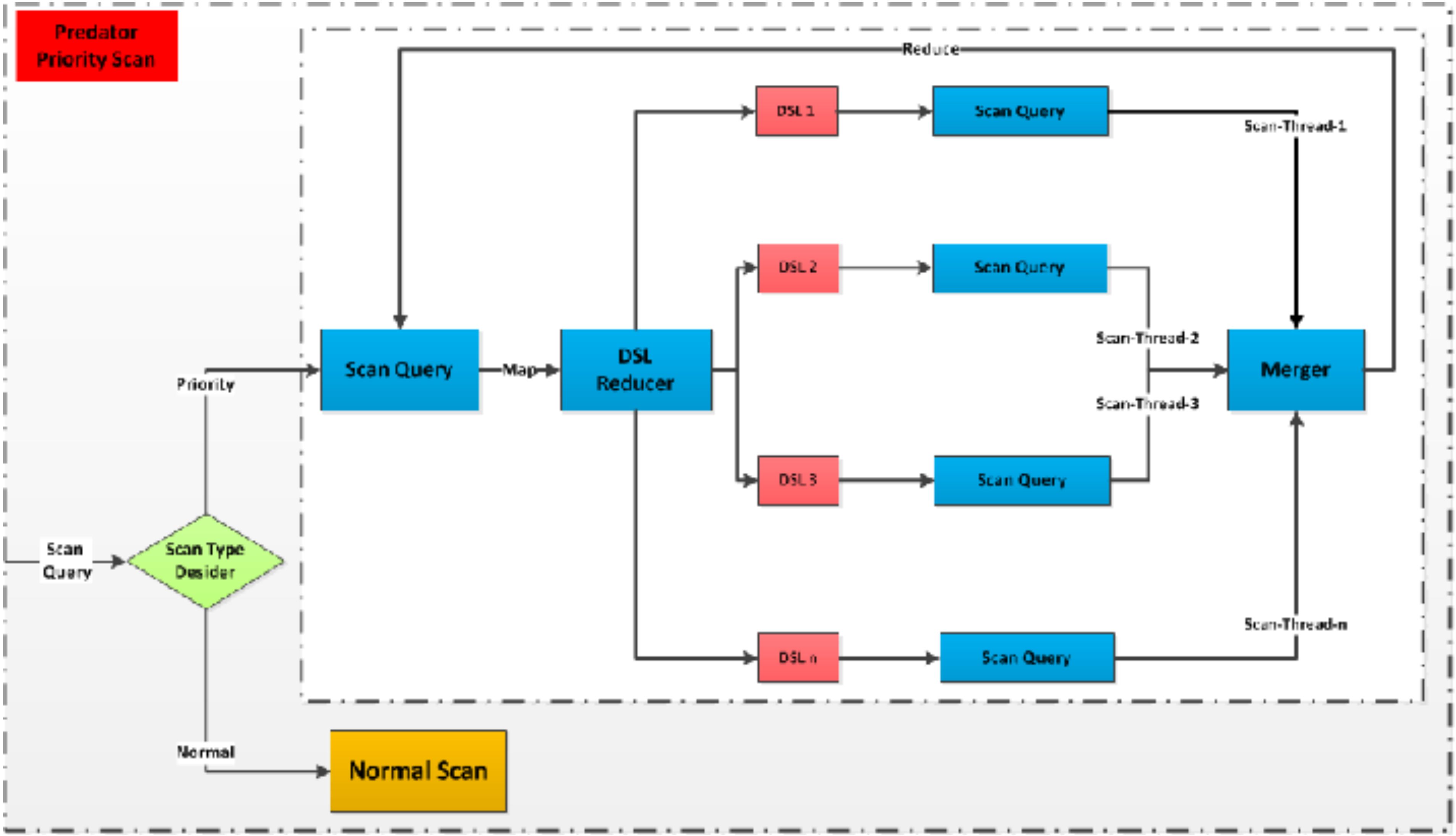
ELK

Q&A

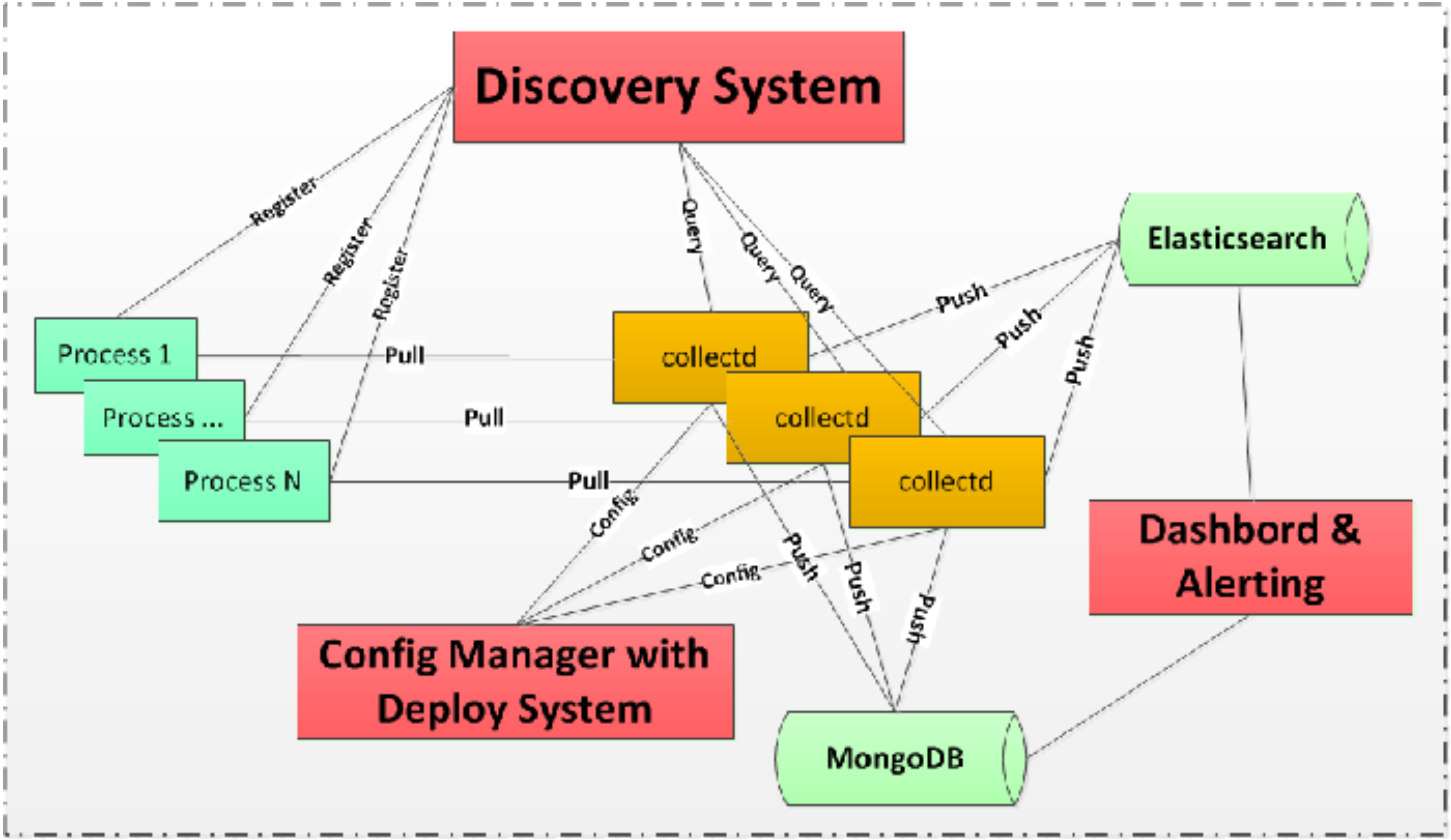
谢谢

Backup Slide

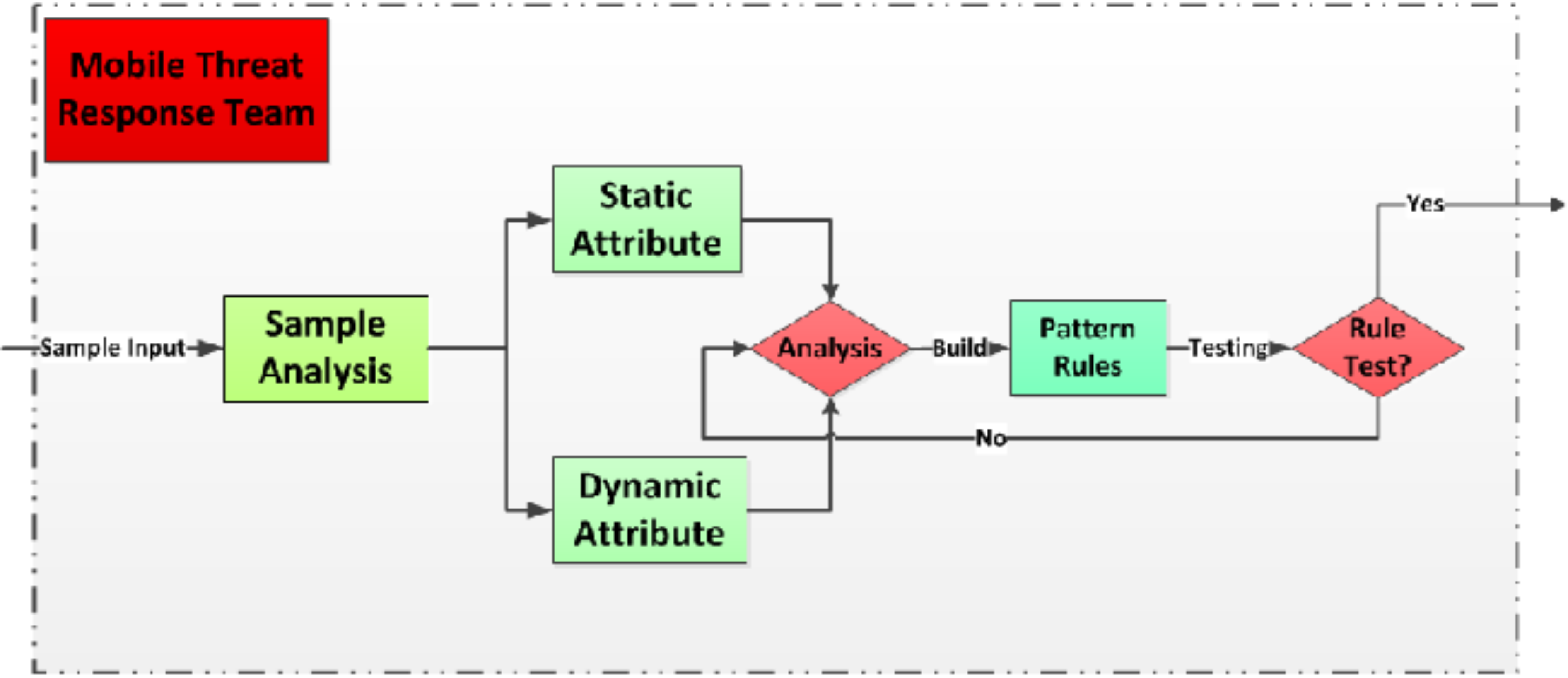
Backup -- Priority Scan



Backup Metrics



Backup 我们做什么？



Backup Pros and Cons -- Partition

我们来讨论下***Pros and Cons***

Pros：

- Code Logical clear.
- Speed up indexing rate.
- Avoid frequently update.
- High available, Scalable which lower down interference.

Cons:

- Not stay in same shard.
- Drop Posting lists join using **bitset** (filter in-memory).
- Drop Posting lists join using **skip-list** (random access disk).
- Need high performance cross cluster/type supporting tool.