# 通用接口

--assetInfo 互联网露报面资产

/assetInfo/list\_AssetInfos

请求参数page\_size,page\_num,*department,*beginTime,*endTime,ip,port,os,timeRange*

/assetInfo/groupByTime

请求参数timeRange[1 HOUR,6 HOUR,1 DAY],size(6),

*department,*beginTime,*endTime,ip,port*

/assetInfo/groupByParm

请求参数groupfields,topn(5),timeRange[1 HOUR,6 HOUR,1 DAY]

*department,*beginTime,*endTime,ip,port*

--Malware 恶意程序URL监测

/Malware/listMalwares

page\_size,page\_num,*city,timeRange*

/Malware/groupByTime

timeRange[1 HOUR,6 HOUR,1 DAY],size(6), *city*

/Malware/groupByParm

groupfields,topn,timeRange[1 HOUR,6 HOUR,1 DAY],*city*

/Malware/groupByParmUnion

groupfields,topn,timeRange[1 HOUR,6 HOUR,1 DAY],*city*

--IndecencyScanResult 敏感词扫描结果

/IndecencyScanResult/listScanResults

page\_size,page\_num,*beginTime*,*endTime,oriurl,ip,port,department,url,sensitype,occurence,timeRange，vulnerable[‘true’]*

/IndecencyScanResult/groupByTime

timeRange[1 HOUR,6 HOUR,1 DAY],size(6),*department*

/IndecencyScanResult/groupByParm

groupfields,topn,timeRange[1 HOUR,6 HOUR,1 DAY],*beginTime*,*endTime,oriurl,ip,port,department,url,*

--srvResource 端口服务开放

/srvResource/listSrvRes

page\_size,page\_num,*department，beginTime*,*endTime,ip,port,service，isRegisted[‘true’],vulnerable[‘[’true’]*

/srvResource/groupByTime

timeRange[1 HOUR,6 HOUR,1 DAY,6 MONTH],size(6),*department,isRegisted[‘true’],vulnerable[‘true’]*

/srvResource/groupByParm

groupfields,topn,timeRange[1 HOUR,6 HOUR,1 DAY,6 MONTH],*department,isRegisted[‘true’],vulnerable[‘true’]*

--Vulnerability 漏洞

/Vulnerability/listVulnerabilitys

page\_size,page\_num,*timeRange,beginTime*,*endTime,ip,port,department,service,vulstatus[0,1]*

/Vulnerability/groupByTime

timeRange[1 HOUR,6 HOUR,1 DAY],size(6),*beginTime*,*endTime,ip,port,department,service,vulstatus[0,1]*

/Vulnerability/groupByParm

groupfields,topn,timeRange[1 HOUR,6 HOUR,1 DAY], *beginTime*, *endTime, ip, port, department, service, vulstatus[0,1]*

# 首页

## 1，资产总量/有漏洞的资产总量 按月分组统计

总量

/srvResource/groupByTime

入参：时间范围timeRange(6 MONTH)，分组数量size(默认6)，部门department(默认是全省，模糊匹配)

结果：各个时间段的统计量

查询逻辑：按服务ip端口表的创建时间分组统计

有漏洞的

/srvResource/groupByTime

入参：时间范围timeRange(6 MONTH)，分组数量size(默认6)，部门department(默认是全省，模糊匹配)，是否有漏洞vulnerable ('true')

结果：各个时间段的统计量

查询逻辑：

有漏洞的资产总量：关联服务ip端口表和漏洞表中未修复（漏洞状态为1）的记录数量，ip+端口为一条资产，按服务ip端口表的创建时间分组统计。

## 2，已报备/未报备有漏洞的资产总量 按月分组统计

有漏洞的总量

/srvResource/groupByTime

入参：时间范围timeRange(6 MONTH)，分组数量size(默认6)，部门department(默认是全省，模糊匹配)，是否有漏洞vulnerable ('true')

结果：各个时间段的统计量

查询逻辑：

有漏洞的资产总量：关联服务ip端口表和漏洞表中未修复（漏洞状态为1）的记录数量，ip+端口为一条资产，按服务ip端口表的创建时间分组统计。

未报备有漏洞

/srvResource/groupByTime

入参：时间范围timeRange(6 MONTH)，分组数量size(默认6)，部门department(默认是全省，模糊匹配)，是否有漏洞vulnerable ('true') ，是否报备*isRegisted*('true')

结果：各个时间段的统计量

查询逻辑：

有漏洞已报备的资产总量：关联服务ip端口表和漏洞表中未修复（漏洞状态为1）的记录数量，ip+端口为一条资产，同时关联ip段分配表和互联网暴露表，按服务ip端口表的创建时间分组统计。

已报备，ip能在ip表及互联网暴露表中能查到的

未报备，用有漏洞的总量减去已报备的

## 3，告警信息 按时间分组统计

/IndecencyScanResult/groupByTime

入参：时间范围timeRange(1 HOUR,6 HOUR,1 DAY)，分组数量size(默认6)，部门*department* (默认是全省，模糊匹配)

结果：各个时间段的统计量

查询逻辑：按时间条件查询敏感词扫描结果表中的记录数，并关联资产暴露表统计有多少个网站

## 4，不良网站量

同3

## 5，恶意软件量 按时间分组统计

/Malware/groupByTime

入参：时间范围timeRange(1 HOUR,6 HOUR,1 DAY)，分组数量size(默认6)，部门city(默认是全省，模糊匹配)

结果：各个时间段的统计量

查询逻辑：到恶意程序表按捕获时间统计恶意软件

## 6，各地市数据统计

如下多个接口

入参：时间范围

结果：时间范围内，各地市数据统计明细

查询逻辑：

各地市不良网站量/全省不良网站量 按扫描时间筛选

/IndecencyScanResult/groupByAsset

/IndecencyScanResult/listScanResults

各地市恶意软件量/全省恶意软件量

/Malware/groupByParm

各地市有漏洞的资产总量/全省有漏洞的资产总量

/Vulnerability/groupByParm /Vulnerability/listVulnerabilitys

各地市未报备存在漏洞资产量/全省未报备存在漏洞资产量

/srvResource/listSrvRes

isRegisted ('true','false' ) +vulnerable ('true','false' )

# 资产监测

## 1，历史总量

/srvResource/listSrvRes

入参：page\_size,page\_num

结果：所有资产量

查询逻辑：

端口服务开放情况表所有的数据

2，近半年新增资产量

/srvResource/listSrvRes

入参：时间范围beginTime,*endTime*，page\_size,page\_num

结果：近半年新增资产量

查询逻辑：

端口服务开放情况表创建时间在时间范围内的数据

## 3，近半年新增已报备未报备资产量

/srvResource/listSrvRes

入参：时间范围beginTime,*endTime*，page\_size,page\_num，*isRegisted*('true')

结果：近半年已报备新增资产量

查询逻辑：

端口服务开放情况表创建时间在时间范围内的数据，同时关联ip分段表和互联网暴露面表能查询到的。

未报备的用2获取到的总数-3获取到的已报备的资产量

## 4，近半年资产所属部门分析 按字段分组统计

/srvResource/groupByParm

入参：时间范围beginTime,*endTime*，分组数量topn(默认5)，地市 *department*,分组字段groupfields(*department*)

结果：各个所属部门的统计量

查询逻辑：

通用按字段分组统计

## 5，近半年资产开放服务分析 按字段分组统计

/srvResource/groupByParm

入参：时间范围beginTime,*endTime*，分组数量topn(默认5)，地市 *department*,分组字段groupfields(*service*)

结果：各个服务类型的统计量

查询逻辑：

通用按字段分组统计

## 6，近半年资产端口分析 按字段分组统计

/srvResource/groupByParm

入参：时间范围beginTime,*endTime*，分组数量topn(默认5)，地市*department*,分组字段groupfields(*port*)

结果：各个端口的统计量

查询逻辑：

通用按字段分组统计

## 7，漏洞类型分析 按漏洞类型分组统计

/Vulnerability/groupByParm

入参：时间范围timeRange(1 HOUR,6 HOUR,1 DAY)，分组数量topn(5),，地市*department ，分组字段*groupfields*（vulname）*

结果：各个时间段出现漏洞按类型分组统计

查询逻辑：

漏洞表中按刷新时间过滤。

## 8，漏洞状态分析 按漏洞状态分组统计

/Vulnerability/groupByParm

入参：时间范围timeRange(1 HOUR,6 HOUR,1 DAY)，分组数量topn(5),，地市*department ，分组字段*groupfields*（vulstatus）*

结果：各个时间段出现漏洞按是否修复分组统计

查询逻辑：

漏洞表中按刷新时间过滤。

## 9，漏洞类型分析 按时间分组统计

漏洞量

/Vulnerability/groupByTime

入参：时间范围timeRange(1 HOUR,6 HOUR,1 DAY)，分组数量size(默认6)，地市*department* ,

结果：各个时间段有漏洞的资产的统计量

查询逻辑：

按刷新时间过滤查询漏洞表查询，进行时间分组

修复漏洞量

/Vulnerability/groupByTime

入参：时间范围timeRange(1 HOUR,6 HOUR,1 DAY)，分组数量size(默认6)，地市*department* , *vulstatus=(1 ，0)* 查询漏洞的传1，查询漏洞修复的传0

结果：各个时间段修复的漏洞的统计量

查询逻辑：

按刷新时间过滤查询漏洞表查询，进行时间分组

修复率= 修复量/漏洞量

# 不良信息

## 1，不良网页总量，同时存在漏洞网页量

/IndecencyScanResult/listScanResults

入参：时间范围，page\_size,page\_num，是否存在漏洞vulnerable ('true' )

结果：按条件统计数量

查询逻辑：

到敏感词扫描结果表按时间获取网页总数

根据敏感词扫描结果表中关联的暴露面资产表，及漏洞表，关联查询符合条件的ip+端口数量

## 2，趋势分析 按时间分组统计

/IndecencyScanResult/groupByTime

入参：timeRange(1 HOUR,6 HOUR,1 DAY)，分组数量size(默认6)，地市*department*

结果：各个时间段存在敏感词的网页数量

查询逻辑：

到敏感词扫描结果表按时间分组查询

## 3，不良信息类型对比 按字段分组统计

/IndecencyScanResult/groupByParm

入参：时间范围timeRange(1 HOUR,6 HOUR,1 DAY)，分组数量topn，地市*department* ，分组字段groupfields(sensitype)

结果：扫描到的敏感词按类型统计

查询逻辑：

到敏感词扫描结果表获取扫描到的敏感词，然后到敏感词表里获取类型，然后统计各个类型总量

## 4，不良网站所属部门 按字段分组统计

/IndecencyScanResult/groupByAsset

入参：时间范围timeRange(1 HOUR,6 HOUR,1 DAY)，分组数量topn，分组字段groupfields(department)

结果：存在敏感词的网页 按资产所属部门分组统计

查询逻辑：

根据敏感词扫描结果表中关联的暴露面资产表，关联查询按资产所属部门分组统计

# 恶意软件

## 1，恶意软件量:

/Malware/listMalwares

参数:时间范围timeRange(1 HOUR,6 HOUR,1 DAY)，地市*city，*page\_size,page\_num  
结果: 时间段内恶意软件总数

## 2，恶意软件量 按时间分组

-----/Malware/getByName  
参数:  
 时间段(timeRange),

分组数量(size),  
 地区(city)  
结果: 各时间段的数据量  
逻辑:  
 table:malware  
 根据时间段及恶意软件md5去malware表中查询记录,且相同md5算作一个软件,统计时间段内出现的恶意软件的数量.

## 3，感染用户top10病毒软件

---/malware/groupByParm  
参数:  
 时间段(timeRange),  
 地区(city),  
 分组数量(topn)

分组字段groupfields(name)

结果: 各个病毒软件数量  
逻辑:  
 table:malware  
 根据病毒名称进行分组查询记录数

## 4. 病毒软件属性占比:

---/malware/groupByParm

参数:  
 时间段(timeRange),  
 地区(city),  
 分组字段groupfields(attrubite)

分组数量(topn)  
结果: 各时间段的病毒占比数据  
逻辑:  
  table:malware  
  根据病毒属性进行分组查询记录数.

## 5. 感染用户号码归属地分析:

---/malware/groupByParm

参数:  
 时间段(timeRange)  
 地区(city),  
 分组数量(size),  
 手机号groupfields(city)  
结果: 各时间段的归属地数据量展示  
逻辑:  
  table:malware  
  根据时间条件及手机号去恶意软件表中查询与之对应的归属地区记录    "name":"A.Payment.tatic.d",

## 6. 感染用户病毒软件挖掘分析:

---/malware/groupByTime

参数:  
 时间段(timeRange)  
 分组数量(size),  
 地区(city)  
 病毒名称(name)  
结果: 各时间段的数据分析  
逻辑:  
  table:malware  
  根据时间条件进行分组查询指定病毒名称的记录数 

恶意软件控制量和下载量业务

## 1.恶意URL控制量:

  ----/Malware/getByURL

参数:  
 时间段(timeRange),  
 分组数量(size),  
 地区(city)  
结果: 各时间段的数据量  
逻辑:  
 table:malwareControl  
 根据时间段及恶意软件url去表中查询记录,并且按url去重,相同url记为1条，统计时间段内出现的控制的url数量.

## 2.恶意URL下载量:

  ----/Malware/getLoadURL  
参数:  
 时间段(timeRange),  
 分组数量(size),  
 地区(city)  
结果: 各时间段的数据量  
逻辑:  
 table:malwareDownload  
 根据时间段及恶意软件url去表中查询记录,并且按url去重,相同url记为1条，统计时间段内出现的下载的url数量.

## 3.恶意软件属性图:

/Malware/groupByParmUnion

参数: 时间段, 地区, 分组字段groupfields(attribute)  
结果: 按病毒属性字段分组统计  
逻辑:

malwareControl malwareDownload

根据时间段及地市条件去两个表中查询所有记录

## 4.控制IP:

----目前写死的固定数值

参数: 时间段, 地区, 分组数量  
结果: 各时间段的数据分析  
逻辑:根据时间条件进行分组查询记录数并分组统计

## 5.感染用户号码归属地分析:

---/Malware/groupByParmUnion  
参数:  
 时间段(timeRange),  
 地区(city),  
 分组字段groupfields(city)  
结果: 各手机号码的归属地分组统计  
逻辑:  
  malwareControl malwareDownload

根据时间段及地市条件去两个表中查询所有记录并分组统计

## 1，恶意软件Control，Download:

/Malware/listMalwareEvent

参数:时间范围timeRange(1 HOUR,6 HOUR,1 DAY)，地市*city，*page\_size,page\_num  
结果: 时间段内恶意软件control和download的详细列表

6.铁通资产:

1.获取列表：

---/CRCassetInventory/listCRCAsset

入参：时间范围，page\_size,page\_num

结果：获取铁通资产列表

查询逻辑：

实现分页查看数据列表。

2.按字段分组统计：

---/CRCassetInventory/groupByParm   
参数:  
 时间段(timeRange),  
 地区(department),  
 分组字段groupfields(department)  
结果: 各归属地分组统计  
逻辑:

根据时间段及地市条件去表中查询所有记录并分组统计

3.统计铁通资产量：

---/CRCassetInventory/getCountAssert  
参数:  
 时间段(timeRange),  
结果: 各归属地分组统计  
逻辑:

根据时间段及地市条件去表中查询所有记录并统计记录

7. 终端资产:

1.获取列表：

---/terminalSecurity/listTerminalSecurity

入参：时间范围，page\_size,page\_num

结果：获取终端资产列表

查询逻辑：

实现分页查看数据列表。

2.按字段分组统计：

---/terminalSecurity/groupByParm   
参数:  
 时间段(timeRange),  
 分组字段groupfields(position)  
结果: 各归属地分组统计  
逻辑:

根据时间段及地市条件去表中查询所有记录并分组统计

3.统计终端资产日志分类量，且统计补全返回值0：

---/terminalSecurity/groupByMulParm  
参数:  
 时间段(timeRange),

分组字段groupfields：logcategory position  
结果: 各归属地分组统计   
逻辑:

根据条件去表中查询日志分类记录并分组统计城市对应记录