目录

威胁情报(KTI)OpenAPI概览

API版本Version 2019-07-11

威胁情报(KTI)相关接口

接口功能	Action Name	功能描述
查询威胁情报	SearchIntelInfo	查询威胁情报，支持IP和域名查询

请求结构

客户调用金山云威胁情报服务(KTI)的openAPI接口是通过向指定服务地址发送请求，并按照openAPI文档说明在请求中添加相应的公共参数和接口参数来完成的。

威胁情报(KTI)openAPI的请求结构组成如下：

1. 服务地址

威胁情报的服务接入地址为：ksm.api.ksyun.com

2. 通信协议

支持通过 HTTP 或 HTTPS 两种方式进行请求通信，推荐使用安全性更高的 HTTPS方式发送请求。

3. 请求方法

威胁情报(KTI)的openAPI同时支持GET和POST请求，推荐使用GET请求方式。

注意

- 不能混合使用两种请求方式。如果使用 GET 方式，参数均从 querystring 取得；如果使用 POST 方式，参数均从 请求Body中取得
- 如果请求方式是GET，需要对所有请求参数做URL编码；如果请求方式是POST，需要使用x-www-form-urlencoded方式进行编码。

4. 请求参数

金山云openAPI请求包含两类参数：公共请求参数和接口请求参数。其中，公共请求参数是每个接口都要用到的请求参数，具体可参见公共参数与签名机制小节；接口请求参数是各个接口所特有的，具体见各个接口的“请求参数”描述。

5. 字符编码

请求及返回结果都使用utf-8进行编码。

返回结果

返回结果

调用金山云的openAPI服务，调用成功，返回的HTTP状态码（Status）为200；调用失败，返回4xx 或5xx的HTTP状态码（Status）。

金山云的**威胁情报(KTI)**服务的调用返回的数据格式支持xml和json两种，默认返回xml格式，可通过设置HTTP Header Accept=application/json来改变返回数据格式。

调用成功

xml格式示例

```
<?xml version="1.0" encoding="UTF-8"?>
<response>
    <RequestId>0717e32b-e5b9-9c05-08c1-55b795ea2bed</RequestId>
    </ResponseMetadata>
    <!--返回结果数据-->
</response>
```

json格式示例

```
{
    "RequestId": "4C467B38-3910-447D-87BC-AC049166F216"
    /*返回结果数据*/
}
```

调用失败

调用接口失败，不会返回结果数据；HTTP请求返回一个4xx或5xx的HTTP状态码，返回的HTTP消息体中包含具体的错误代码(code)及错误信息(message)；与调用成功一样还包含请求ID(RequestId)，在调用方找不到错误原因时，可以联系金山云客服，并提供RequestId，以便我们尽快帮您解决问题。

xml格式示例

```
<?xml version="1.0" encoding="UTF-8"?>
<response>
<Error>
<Code>PermissionDenied</Code>
<InnerCode>permission_denied</InnerCode>
<Message>权限不足</Message>
</Error>
<RequestId>fd229f7c-e65f-1402-1d85-8cdff25c8b59</RequestId>
</response>
```

json格式示例

```
{
"Error": {
"Code": "PermissionDenied",
"InnerCode": "permission_denied",
"Message": "权限不足"
},
"RequestId": "0717e32b-e5b9-9c05-08c1-55b795ea2bed"
}
```

公共错误

错误代码(Code)	错误消息(Message)	HTTP 状态码	中文描述（语义）
MissingAuthenticationToken	Request is missing 'Host' header.	403	请求header中缺少Host
MissingAuthenticationToken	Request is missing Authentication Token.	403	请求header中缺少认证token
MissingAuthenticationToken	%s not in Http Header.	403	%s不在Http header中
SignatureDoesNotMatch	Host' must be a 'SignedHeader' in the Authorization.	403	请求的SignedHeader中必须包含Host
SignatureDoesNotMatch	Credential should be scoped with a valid terminator: 'aws4_request', not: %s.	403	请求Authorization header中的“Credential”末尾必须是“aws4_request”
SignatureDoesNotMatch	Credential should be scoped to a valid region, not:%s.	403	请求Authorization header中的“Credential”中的Region信息无效
SignatureDoesNotMatch	Credential should be scoped to correct service: %s.	403	请求Authorization header中的“Credential”中的Service信息无效
SignatureDoesNotMatch	The request signature we calculated does not match the signature you provided.	403	请求中提供的签名与实际计算结果不匹配
SignatureDoesNotMatch	Signature expired:%s.	403	签名已过期
SignatureDoesNotMatch	Date in Credential scope does not match YYYYMMDD from ISO-8601 version of date from HTTP.	403	请求Authorization header中的“Credential”中的Date应该是ISO8601基本格式，形如”YYYYMMDD“
InvalidClientTokenId	The security token included in the request is invalid.	403	请求中提供的AccessKeyId无效

AccessDenied	User: %s is not authorized to perform: %s.	403	用户%s无权限操作该资源：%s
IncompleteSignature	Date must be in ISO-8601 'basic format'. Got '%s'. See http://en.wikipedia.org/wiki/ISO_8601.	400	Date必须符合ISO_8601基本格式，参考：http://en.wikipedia.org/wiki/ISO_8601
IncompleteSignature	KSC query-string parameters must include %s. Re-examine the query-string parameters.	400	查询条件中缺少签署信息，查询条件中必须包含”X-Amz-Algorithm“、”X-Amz-Credential“、”X-Amz-SignedHeaders“、”X-Amz-Date“信息
IncompleteSignature	Unsupported ksc 'algorithm': %s.	400	只支持如下签名算法：AWS4-HMAC-SHA256
IncompleteSignature	Authorization header requires 'Credential' parameter. Authorization=%s.	400	请求Authorization header中需要包含“Credential”参数
IncompleteSignature	Credential must have exactly 5 slash-delimited elements, e.g. accesskeyid/date/region/service/aws4_request, got: %s.	400	请求Authorization header中中“Credential”至少包含5项以斜杠分隔的元素，如：keyid/date/region/service/aws4_request
IncompleteSignature	Authorization header format error.	400	请求Authorization header的格式错误
IncompleteSignature	Authorization header requires existence of either a 'X-Amz-Date' or a 'Date' header, Authorization=%s	400	请求中缺少“X-Amz-Date”或者“Date” header信息
IncompleteSignature	Authorization header requires 'Signature' parameter. Authorization=%s	400	请求Authorization header中缺少“Signature”信息
IncompleteSignature	Authorization header requires 'SignedHeaders' parameter. Authorization=%s	400	请求Authorization header中缺少“SignedHeaders”信息
ServiceUnavailable	Exception %s	500	服务暂不可用
ServiceUnavailable	Auth Service is unavailable because of an unknown error, exception or failure	500	验签或授权服务暂不可用
ServiceUnavailable	Request was rejected because it referenced an 'InnerApi' that does not have an internal service	404	请求被拒绝，因其引用的InnerAPI无内部服务。
ServiceUnavailable	OpenAPI or Service is unavailable because of an unknown error, exception or failure.	500	openAPI或服务暂不可用。
DryRunOperation	Request would have succeeded, but DryRun flag is set	412	请求本可成功，但由于设置DryRun标记未成功
NoSuchEntity	Request was rejected because it referenced an 'InnerApi' that does not exist.	404	请求被拒绝，因其引用的InnerAPI不存在
LimitExceeded	Request was rejected because the request speed of this openAPI is beyond the current flow control limit.	409	请求被拒绝，因该openAPI接口访问速度已达到流控上限
InvalidParameterValue	An invalid or out-of-range value was supplied for the input parameter %s.	400	输入参数%s的值无效、不合法或者超出范围
InvalidMethod	The method %s for is not valid for this web service.	400	Method %s对当前web服务无效
MissingParameter	An value must be supplied for the input parameter %s.	400	输入参数 %s的值不能为空
InvalidQueryParameter	The query parameter %s is malformed or does not adhere to KSC standards.	400	查询参数 %s格式不对、不存在或者不符合金山云标准
ServiceTimeout	Internal Service is unavailable because of time out.	500	内部服务由于超时暂不可用

公共参数与签名机制

金山云OpenAPI支持以下两种签名算法，您可以根据业务需要选择所使用的签名算法，请注意两种签名算法所使用的公共参数有所区别。

（1）简化版签名算法，相比AWS签名算法，签名机制更加简单。

- 公共参数
- 签名算法

（2）AWS签名算法版本4，具体可以参考AWS文档

IP信息

IntelIpInfo（威胁情报查询Ip信息）

Contents（内容）

Ip

- ip地址
- 类型：String
- 是否可缺省：否

Carrier

- 运营商
- 类型：String
- 是否可缺省：是

Location

- 位置信息
- 类型：IpLocationInfo
- 是否可缺省：是

Asn

- ASN信息
- 类型：IpAsnInfo
- 是否可缺省：是

Judgments

- 威胁类型
- 类型：String list
- 是否可缺省：是
- 取值范围：威胁类型全集

Tags

- 威胁标签
- 类型：TagInfo list
- 是否可缺省：是

威胁类型中英文对应表

英文名称（不区分大小写）	中文名称
C2	远控
Botnet	僵尸网络
Hijacked	劫持
Phishing	钓鱼
Malware	恶意软件
Exploit	漏洞利用
Scanner	扫描
Zombie	傀儡机
Spam	垃圾邮件
Suspicious	可疑
Compromised	失陷主机
Whitelist	白名单
Brute Force	暴力破解

Proxy	代理
Info	基础信息

Suspicious（可疑）分类

英文名称（不区分大小写）	中文名称
MiningPool	矿池
CoinMiner	私有矿池

C2（远控）分类

英文名称（不区分大小写）	中文名称
Sinkhole C2	安全机构接管C2

Brute Force（暴力破解）分类

英文名称（不区分大小写）	中文名称
SSH Brute Force	SSH 暴力破解
FTP Brute Force	FTP 暴力破解
SMTP Brute Force	SMTP 暴力破解
Http Brute Force	HTTP AUTH 暴力破解
Web Login Brute Force	撞库

Proxy（代理）分类

英文名称（不区分大小写）	中文名称
HTTP Proxy	HTTP Proxy
HTTP Proxy In	HTTP 代理入口
HTTP Proxy Out	HTTP 代理出口
Socks Proxy	Socks 代理
Socks Proxy In	Socks 代理入口
Socks Proxy Out	Socks 代理出口
VPN	VPN 代理
VPN In	VPN 入口
VPN Out	VPN 出口
Tor	Tor 代理
Tor Proxy In	Tor 入口
Tor Proxy Out	Tor 出口

Info（基础信息）分类

英文名称（不区分大小写）	中文名称
Bogon	保留地址
FullBogon	未启用IP
Gateway	网关
IDC	IDC 服务器
Dynamic IP	动态IP
Edu	教育
DDNS	动态域名
Mobile	移动基站
Search	Engine Crawler 搜索引擎爬虫
CDN	CDN 服务器

IP位置信息

IpLocationInfo（威胁情报查询IP位置信息）

Contents（内容）

Country

- 国家
- 类型：String
- 是否可缺省：是

CountryCode

- 国家代码
- 类型：String
- 是否可缺省：是

Province

- 省份
- 类型：String
- 是否可缺省：是

City

- 城市
- 类型：String
- 是否可缺省：是

Lng

- 经度
- 类型：String
- 是否可缺省：是

Lat

- 纬度
- 类型：String
- 是否可缺省：是

IP ASN信息

IpAsnInfo（威胁情报查询IP ASN信息）

Contents（内容）

Number

- ASN号码
- 类型：Integer
- 是否可缺省：是

Rank

- 风险值
- 类型：Integer
- 是否可缺省：是
- 取值范围：（0~4，越大代表风险越高）

Info

- ASN信息
- 类型：String
- 是否可缺省：是

域名信息

DomainInfo（威胁情报查询域名信息）

Contents（内容）

Domain

- 域名
- 类型：String
- 是否可缺省：否

CurWhois

- 当前whois信息
- 类型：CurWhois
- 是否可缺省：是

CurIps

- 当前解析的ip信息
- 类型：String list
- 是否可缺省：是

Judgments

- 威胁类型
- 类型：String list
- 是否可缺省：是
- 取值范围：威胁类型全集

Tags

- 威胁标签
- 类型：TagInfo list
- 是否可缺省：是

域名Whois信息

CurWhois（威胁情报查询域名Whois信息）

Contents（内容）

RegistrarName

- 域名服务商
- 类型：String
- 是否可缺省：是

NameServer

- 域名服务器（以|分隔）
- 类型：String
- 是否可缺省：是

RegistrantName

- 注册者
- 类型：String
- 是否可缺省：是

RegistrantEmail

- 注册邮箱
- 类型：String
- 是否可缺省：是

RegistrantCompany

- 注册机构
- 类型: String
- 是否可缺省: 是

RegistrantAddress

- 注册地址
- 类型: String
- 是否可缺省: 是

RegistrantPhone

- 注册电话
- 类型: String
- 是否可缺省: 是

CDate

- 注册时间
- 类型: String
- 是否可缺省: 是

UDate

- 更新时间
- 类型: String
- 是否可缺省: 是

EDate

- 过期时间
- 类型: String
- 是否可缺省: 是

Alexa

- Alexa 排名
- 类型: String
- 是否可缺省: 是

标签信息

TagInfo（威胁情报标签信息）

Contents（内容）

Type

- 标签类型
- 类型：String
- 是否可缺省：是
- 取值范围：标签类别对照表

Tags

- 标签
- 类型：String list
- 是否可缺省：是

标签类别中英文对应表

英文名称（不区分大小写） 中文名称

basic	基础标签
gangs	犯罪团伙
industry	相关行业
region	相关区域
security_event	安全事件
virus_family	病毒家族
vulnerability	安全漏洞

查询结果

IntelInfo（威胁情报查询结果）

Contents（内容）

Type

- 结果类型
- 类型：String
- 是否可缺省：否
- 取值范围：ip | domain

RetCode

- 返回代码
- 类型：Integer
- 是否可缺省：否
- 取值范围：0（成功） 1（输入的域名格式不正确） 2（没有查询到数据）

RetMsg

- 返回信息（当RetCode!=0时）
- 类型：String
- 是否可缺省：否

Ip

- ip信息（当Type=ip && RetCode == 0 时）
- 类型：IntelIpInfo
- 是否可缺省：是

Domain

- 域名信息（当Type=domain && RetCode == 0 时）
- 类型：DomainInfo
- 是否可缺省：是

查询威胁情报

SearchIntelInfo（查询威胁情报）

Request Parameters（请求参数）

Param

- 查询参数，支持ip和域名查询
- 类型：String
- 是否可缺省：否
- 说明：不符合ip格式的都当做域名查询，目前只支持ipv4

Response Elements（返回值）

RequestId

- 请求ID
- 类型：String
- 是否可缺省：否

LeftCount

- 查询剩余次数
- 类型：Integer
- 是否可缺省：否

TotalCount

- 查询总次数
- 类型：Integer
- 是否可缺省：否

IntelInfo

- 威胁情报信息
- 类型：IntelInfo
- 是否可缺省：否

Examples（举例）

Sample Request（请求）

```
http://kms.api.ksyun.com
POST
Action=SearchIntelInfo
```

Sample Response（返回）

```
<?xml version="1.0"?>
<response>
    <RequestId>fd229f7c-e65f-1402-1d85-8cdff25c8b59</RequestId>
    <LeftCount>0</LeftCount>
    <TotalCount>2</TotalCount>
    <IntelInfo>
    </IntelInfo>
</response>
```