



绿盟威胁情报中心NTI

绿盟科技版权所有 2019护网专项培训





01 威胁情报概述

02 绿盟科技威胁情报中心NTI

03 NTI提供的服务

01

威胁情报概述

威胁情报概念

威胁情报是基于证据的知识，包括上下文、机制、指标、可能的结果和可操作的建议，涉及资产面临的现有或新出现的威胁或危害，可为主体威胁或危害的响应决策提供依据。



▶▶ 情报的转化



知识的利用具有普遍性，贯穿整个情报转化过程，从数据转化成信息需要知识，从信息转化成情报同样需要知识

02

绿盟科技威胁情报中心NTI

▶▶ NTI概述

 **名称**：绿盟威胁情报中心

 **英文**：NSFOCUS Threat Intelligence

 **缩写**：NTI

 **形态**：SaaS云端部署，公网环境下均可访问

 **NTI Portal网址**

国内站点 <https://nti.nsfocus.com/>

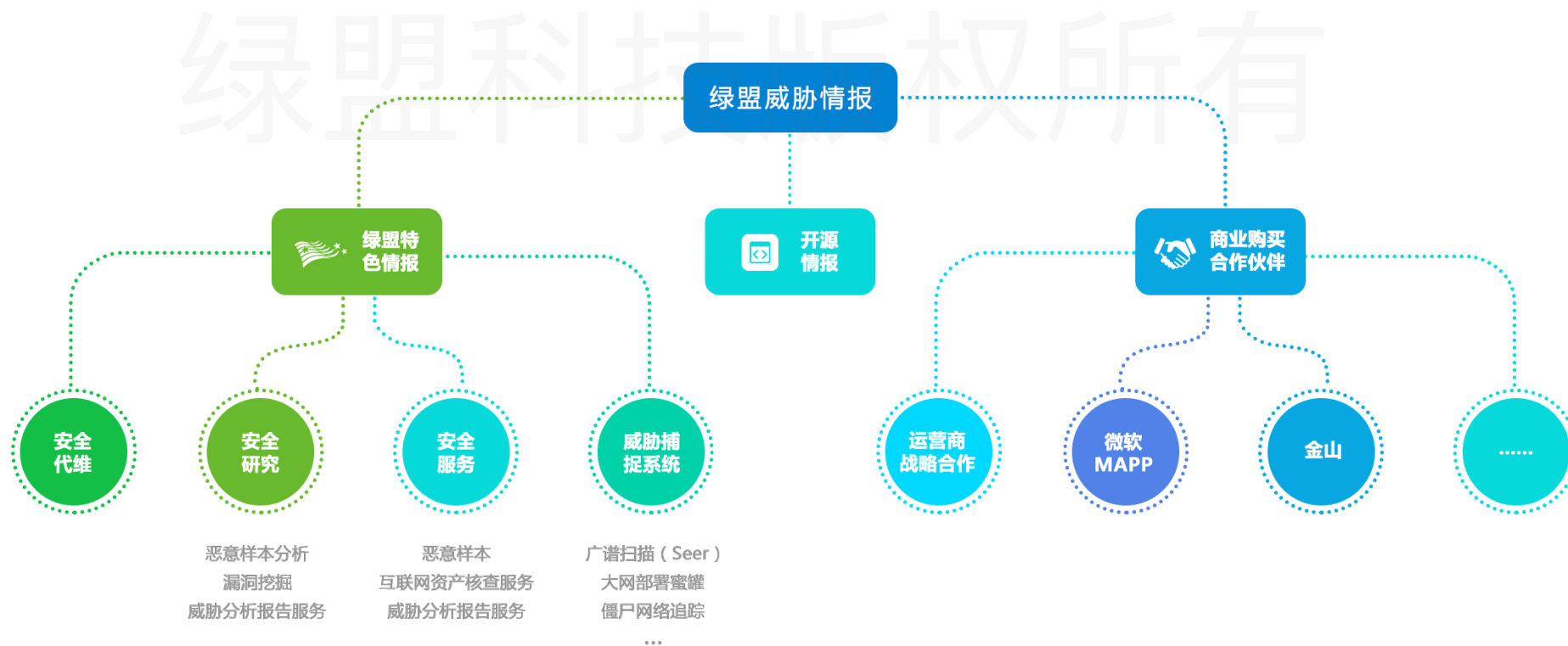
国际站点 <https://nti.nsfocusglobal.com/>

情报数据规格

分类		简要描述	建议用途	数据存量 (单位: 条)	数据增量 (平均) (单位: 条)	
情报数据	威胁类情报 (IOC)	恶意IP库	攻击源IP, 类型包括: DDoS、僵尸主机 (被控端)、利用漏洞攻击、利用恶意软件攻击、Web攻击、扫描源、垃圾邮件源、开设了钓鱼网站等	失陷主机检测、威胁发现和处置、应急响应、攻击溯源、攻击者画像等场景	数千万	万级别/天
		恶意域名库/URL库	恶意域名、恶意URL		数亿	十万级别/天
		恶意样本HASH库	恶意样本的HASH值		数千万	万级别/天
		C&C库	僵尸网络主控端Server地址		数百万	百级别/天
	基础类情报	IP地理信息库	IP归属的国家、省市、经纬度	威胁事件关联分析、攻击溯源、协助进行攻击者画像、网络空间测绘、互联网资产暴露面监控等场景	覆盖全球IP	N/A
		IP资产库	IP开放的端口、服务、运营商归属、banner等		数亿	千万级别/天
		Web资产库	开放了Web服务的资产, 含网页Title、网页内容等		数十亿	百万级别/天
		ASN库	IP所属的ASN		覆盖全球IP	N/A
		PDNS库	IP关联的域名, 域名关联的IP		数百亿	十万级别/天
		whois库	域名的whois信息, 含域名注册邮箱、注册者等		数十亿	十万级别/天
		ICP备案信息库	网站在工信部ICP备案的相关信息, 含备案单位、备案时间、公司名称等		国内所有域名	和ICP备案库保持一致
	网站信息库 (安全舆情)	包含特定关键字 (如企业名称) 的网站Title、页面信息库	用于未知资产发现 (IP、域名、网站) 以及钓鱼网站发现等场景	数亿	百万级别/天	
	漏洞情报	漏洞库	漏洞库	漏洞预警、漏洞闭环管理场景	数十万	数十条/天
	安全资讯	安全资讯库	安全事件的描述、相关联的IOC等	威胁预警等场景	数百条	数条/月
文件分析情报	文件分析库	利用云沙箱对文件进行分析的结果, 含静态分析和动态分析, 可对该文件的行为进行记录和分析。	恶意软件检测和分析等场景	数千万	万级别/天	

▶▶ NTI情报源

绿盟依赖于多年的安全攻防经验，大多数情报数据均为自身生产，因此在情报**独特性**上占据绝对优势。另外也集成了其他**多家商业情报源和开源情报源**。



▶▶ NTI威胁情报种类



▶▶ NTI的特色和独特优势

□ 情报源：

- 绿盟独有的情报源

□ 情报类型：

- 独有的漏洞情报，且能达到小时级更新

□ 情报质量：

- 情报准确可查证，可进行情报回溯（绿盟独有的情报源）

□ 情报使用：

- 绿盟的设备/平台集成了情报模块，可以云地联防

□ 情报标准：

- 参与国标、行标、信工所、工信部等重量级标准制定

03

NTI提供的服务

▶▶ NTI提供的服务

- 互联网资产暴露面核查
- 设备平台联动
- Portal情报查询
- Api接口情报查询
- 威胁情报平台

德盟科技版权所有

基于威胁情报的互联网资产暴露面核查服务



易被攻陷的高危主机

开放了高风险服务端口的主机 (SSH/Telnet/远程桌面/SMB/数据库/.....)
开放了多端口的主机
开放了非常见协议的主机.....



存在恶意行为的主机

发起DDoS攻击/利用漏洞对外发起攻击/扫描源/垃圾邮件源/关联了恶意软件/Botnet客户端.....



值得关注的IP和域名

可能存在业务敏感信息泄露 (对外开放数据库登录页面/web登录没有使用加密协议...)
非有效业务页面



未知资产发现

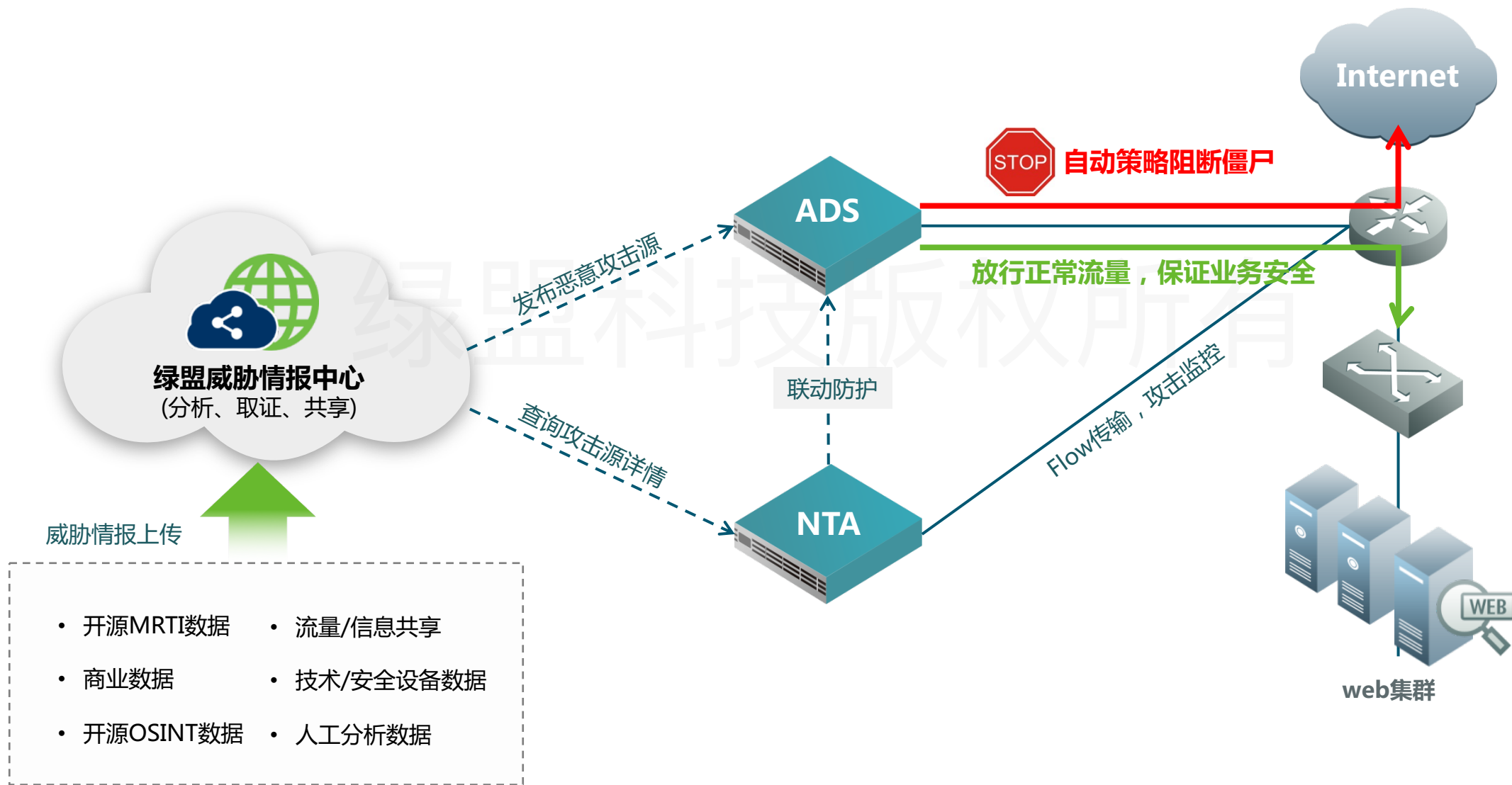
未知IP资产+未知子域名资产



域名是否在工信部ICP备案



▶▶ 绿盟ADS集成威胁情报进行智能抗D



Portal

NSFOCUS 威胁情报中心门户

威胁预警 我的探索 工具 文档 账户: wangchi English

1 输入客户名称、安全事件名称、IP、域名、漏洞名称/编号、文件Hash (MD5/SHA256) 或任意关键字

2 热搜: APT-C1, Wannacry Ransomware, Apache Struts2, Mirai, 193.166.255.171, 82.200.247.240, cnrdn.com, b512812016528580deed32a096d45700
热搜报告: 2018 网络安全观察, 安全事件响应观察报告, 2018 物联网安全年报, 2018 Botnet趋势报告, 2018 DDoS攻击态势报告, IP团伙行为分析, 2017 金融科技安全分析报告, APT-C1

41.63.189.48 扫描IP Lobito, Angola 2019-05-13 16:00:14 GMT

94.21.106.251 扫描IP Budapest, Hungary 2019-05-13 16:00:06 GMT

37.105.103.200 扫描IP Riyadh, Saudi Arabia 2019-05-13 16:00:08 GMT

© 2019 绿盟科技 京公网安备11010802021805 京ICP证110355号

NSFOCUS 威胁情报中心门户

威胁预警 我的探索 工具 文档 账户: wangchi English

帮助

总览

绿盟威胁情报中心 (NTI) 提供针对绿盟科技收集到的最新全网安全资讯与威胁情报, 如资产指纹、漏洞威胁等内容的检索功能, 以及针对检索结果, 提供统计、作图能力。其中, 搜索功能支持按关键字检索和按字段检索两种类型; 并支持检索条件的逻辑运算。

FAQ

- 1. 如何获取NTI Key?**
登录NTI Portal, 单击“账户” > “账户信息”即可查看自己的Key。
- 2. 如何获得NTI API文档?**
打开NTI portal网址, 登录后, 在菜单“文档” > “API”下, 单击“下载API文档”即可获得NTI API文档, 目前版本是NTI-API-V2.1R00F00。
- 3. 如何使用NTI API?**
如果要使用NTI API接口, 首先需要与NTI进行相互认证, 认证通过后方可使用NTI API接口。详细步骤如下:
 - 步骤 1: 向NTI管理控制中心申请授权密钥key。授权密钥key一般为64位长度的字符串, 由NTI统一生成。
 - 步骤 2: 使用密钥key进行认证。每一次接口调用时, 您都需要把申请到的密钥key做为请求头参数发送到API端。提交密钥key使用的参数字段为“NS-NTI-KEY”, 参数值为申请获得的64位字符串。
- 4. NTI API提供哪些功能?**
NTI API提供的功能如下:
 - 单项情报查询, 例如IP情报、域名&URL情报、样本情报、漏洞情报、安全事件情报以及CC情报。
 - 情报模糊搜索, 支持模糊查询。查询关键字将在记录中的所有字段内进行匹配, 并返回被匹配到的数据列表。
 - 情报检索统计, 以查询关键字为基础, 对检索结果的数据进行各种TOP统计。
 - 批量情报下载。
- 5. API调用返回结果显示失败, 怎么分析?**
向NTI API接口发送检索请求后, 返回的数据为状态码时, 表示获取数据失败。常见HTTP状态码如:
 - 200 OK-请求成功。
 - 403 Forbidden-未授权, 认证不通过, 说明: 当key过期时, 返回码为403, 用户可以联系NTI技术支持人员进行处理, 邮箱 nti@nsfocus.com
 - 422 Unprocessable Entity-请求参数错误
 - 500 Internal Server Error-服务器端异常
 - 502 Bad Gateway-服务器端发生未知故障
 - 503 Service Unavailable-由于停机维护或者超载, 服务器暂时无法响应您的请求。
 - 555 数据查询错误
- 6. NTI提供哪些STIX支持?**

javascript:void(0)

IP、域名、
56) 或任意

可查看
亮点③相对

▶▶ API接口

- IP情报
- Domain&URL情报
- 样本情报
- 漏洞情报
- 安全事件情报
- CC情报
- 情报模糊检索
- 情报检索统计

绿盟科技版权所有



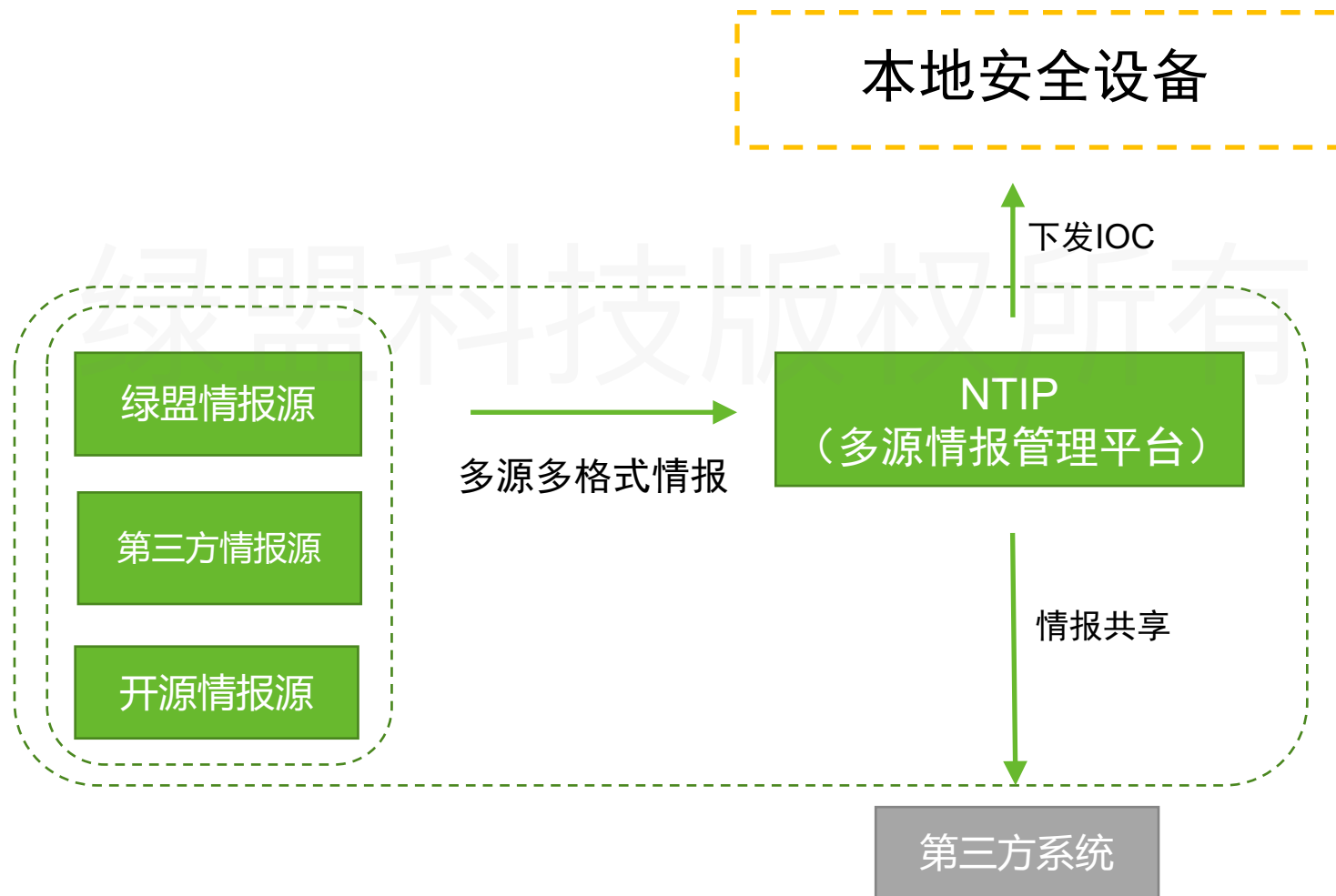
IP情报

```
#!/usr/bin/env python
# -*- coding: utf-8 -*-
import urllib2
import json
import requests
import os
authkey = "xxxxxxxxxxxxxxxxxxxxxxxxx"
api = "https://nti.nsfocus.com/api/v1"
request = urllib2.Request(
    api,
    "",
    {'Content-Type': 'application/json', "N
)
response = urllib2.urlopen(request)
data = json.loads(response.read())
print json.dumps(data)
```

```
{
  "asnInfo": {+ ...},
  "vulInfo": {+ ...},
  "urlInfo": {+ ...},
  "historyInfo": [ ],
  "fileInfo": {+ ...},
  "basicInfo": {
    "province": "California",
    "city": "Mountain View",
    "update_time": "2017-09-11T22:04:09",
    "data_type": "ip",
    "country": "United States",
    "ip_tag": [
      {
        "attribute": "1",
        "attribute_tag": "0"
      },
      {
        "attribute": "0",
        "attribute_tag": "1"
      },
      {
        "attribute": "3",
        "attribute_tag": "2"
      }
    ],
    "updated_time": "2017-09-11T22:04:09",
    "created_time": "2017-09-02T07:00:00",
    "location": "37.40599060058594, -122.0785140991211",
    "country_code": "US",
    "ip": "8.8.8.8",
    "services": [+ ... ],
    "_id": "134744072",
    "os": { },
    "event_tag": [ ]
  }
}
```

e=all"

▶▶ 客户本地威胁情报平台 (**NTIP**)





谢谢！

绿盟科技版权所有

