绿盟威胁情报中心NTI

2019护网专项培训

目录
CONTENTS

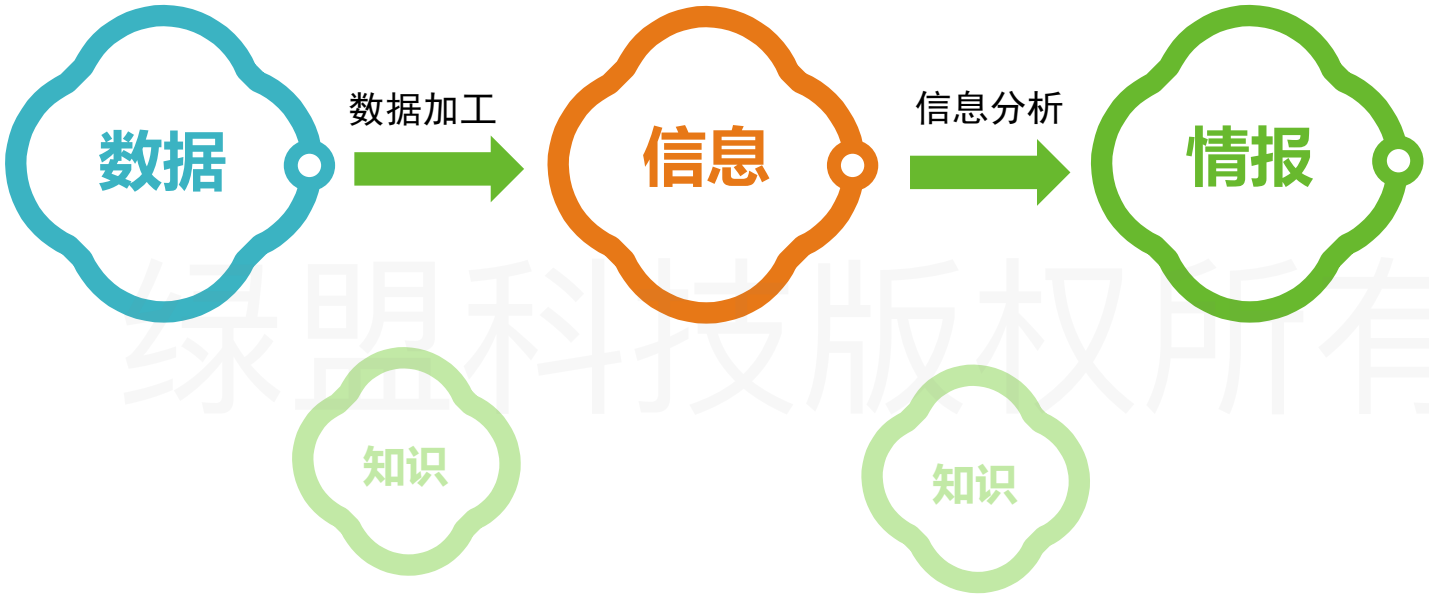
01

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，从数据转化程信息需要知识，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/

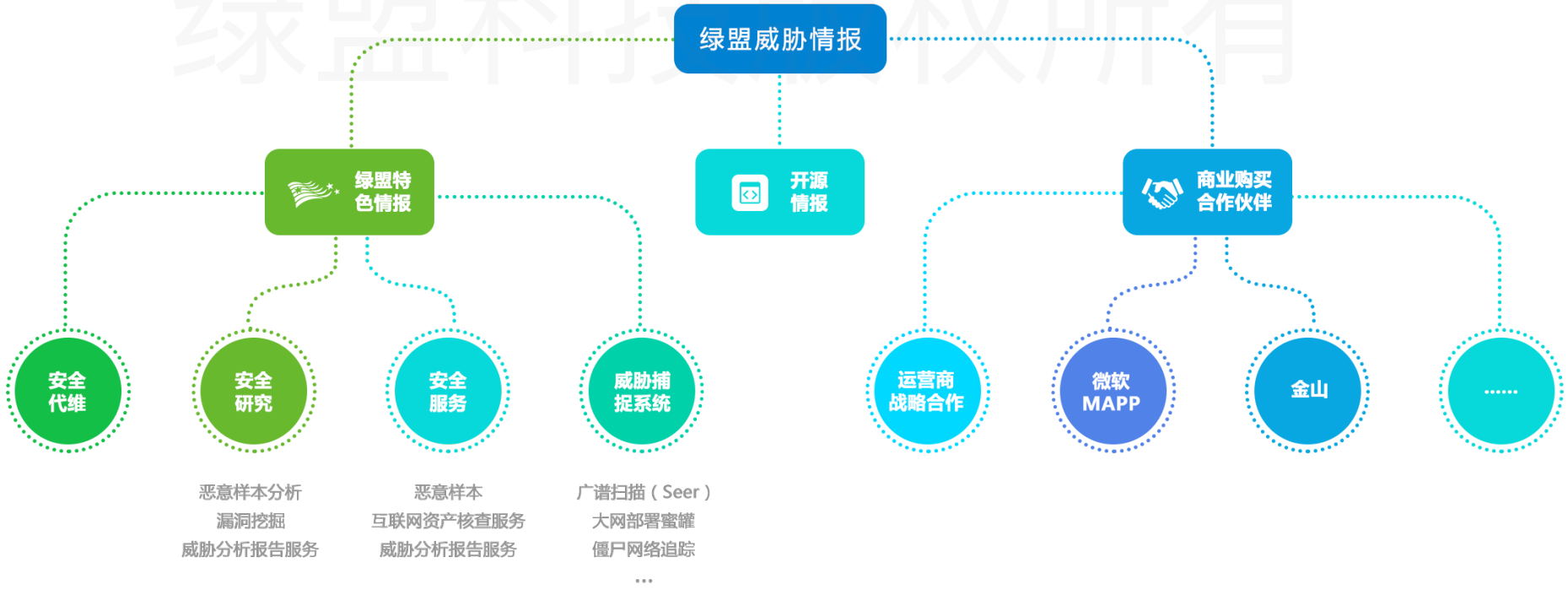
国际站点 https://nti.nsfocusglobal.com/

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

信誉情报

1. 恶意IP
2. 恶意URL
3. 恶意文件
4. C&C

基础信息情报 (IP/域名/URL)

1. IP开放的端口/协议/banner
2. IP所属ASN
3. IP标签（CDN…）
4. 地理信息/所属运营商
5. 是否开放了Web服务
   -通过IP直接访问
   -通过域名访问
6. IP和域名的关联
7. 域名是否备案
   -ICP备案
8. 域名 Whois
9. 子域名发现
10. 域名/URL分类库

漏洞情报

1. 发现时间/更新时间
2. CVE/CNVD/CNNVD ID
3. 厂商/产品
4. 影响版本
5. 解决方案
6. 官方补丁链接
7. 风险级别/热度
8. 是否有POC

威胁事件

1. 事件名称及概述
2. 关联的IP
3. 关联的域名
4. 关联的FileHash
5. 关联的CVE漏洞
6. 相关链接

恶意样情报

1. 恶意样本Hash
2. 样本活动过程
3. 风险等级

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

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


NSFOCUS

基于绿盟威胁情报的
互联网资产暴露面稽查报告

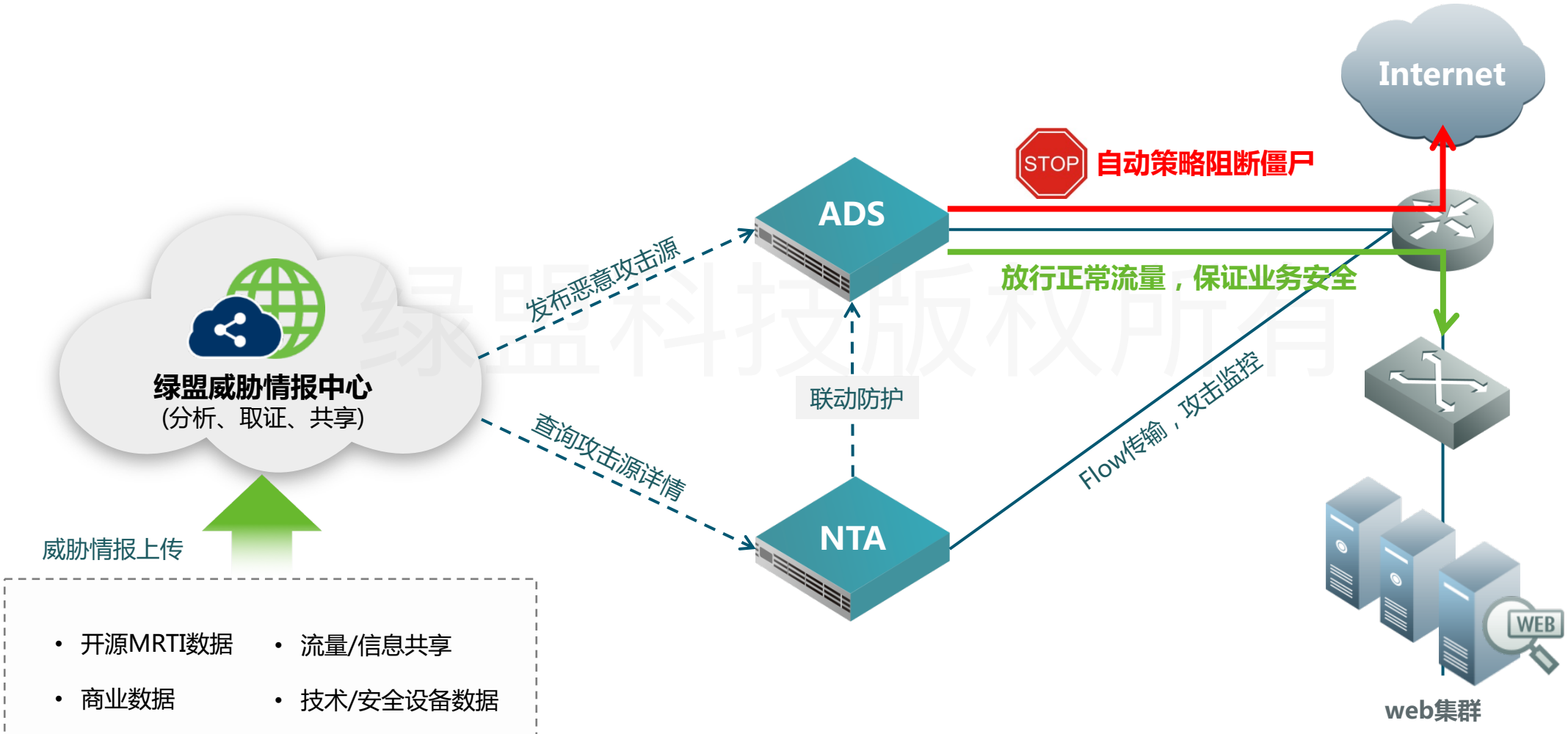
■ 客户名称	银行	■ 密级	商业机密
■ 版本编号	V1.0	■ 日期	2017 年 10 月 15 日

NSFOCUS

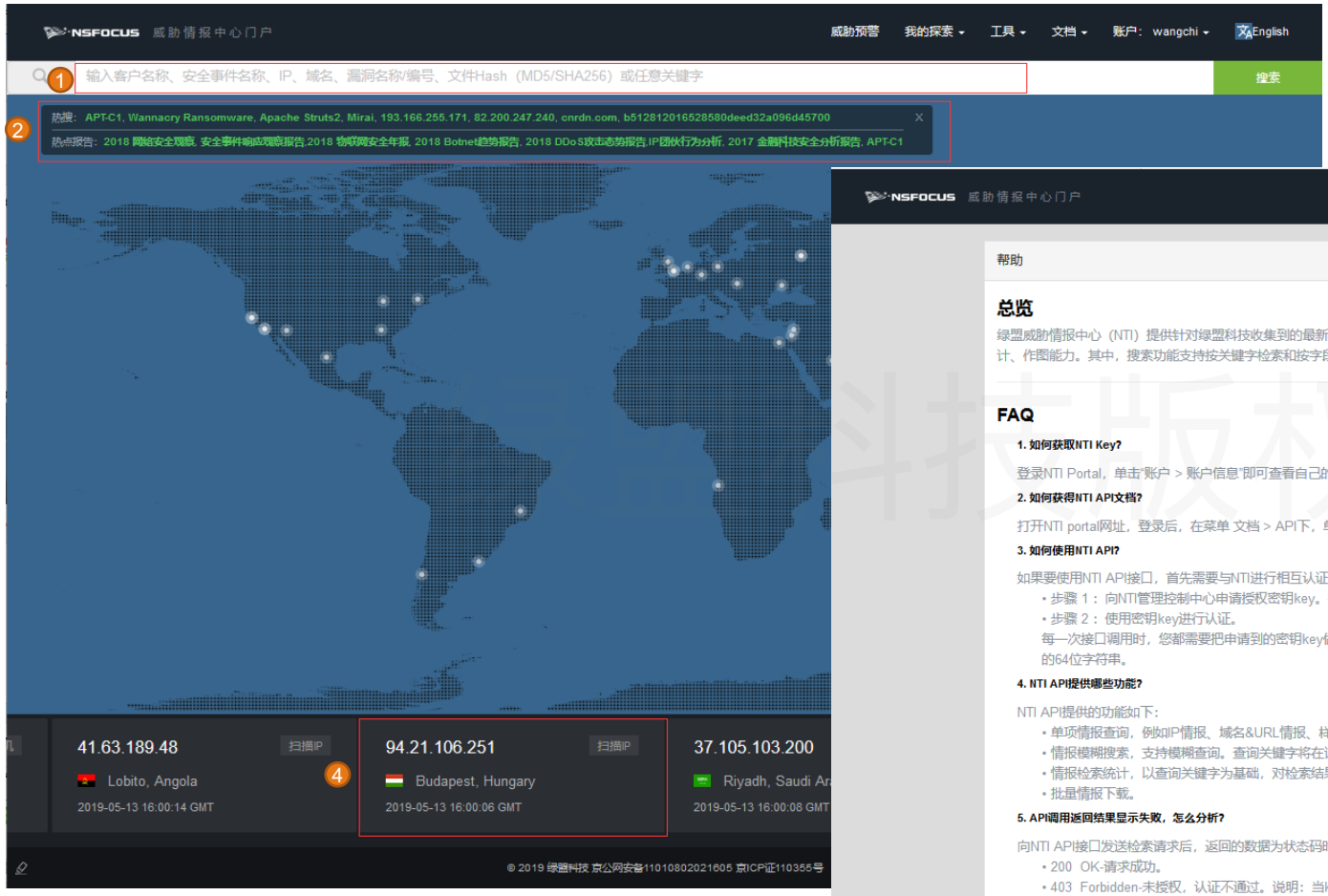
© 2017 绿盟科技

■ 版权声明

绿盟ADS集成威胁情报进行智能抗D



Portal



IP、域名、
56）或任意

]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

IP情报

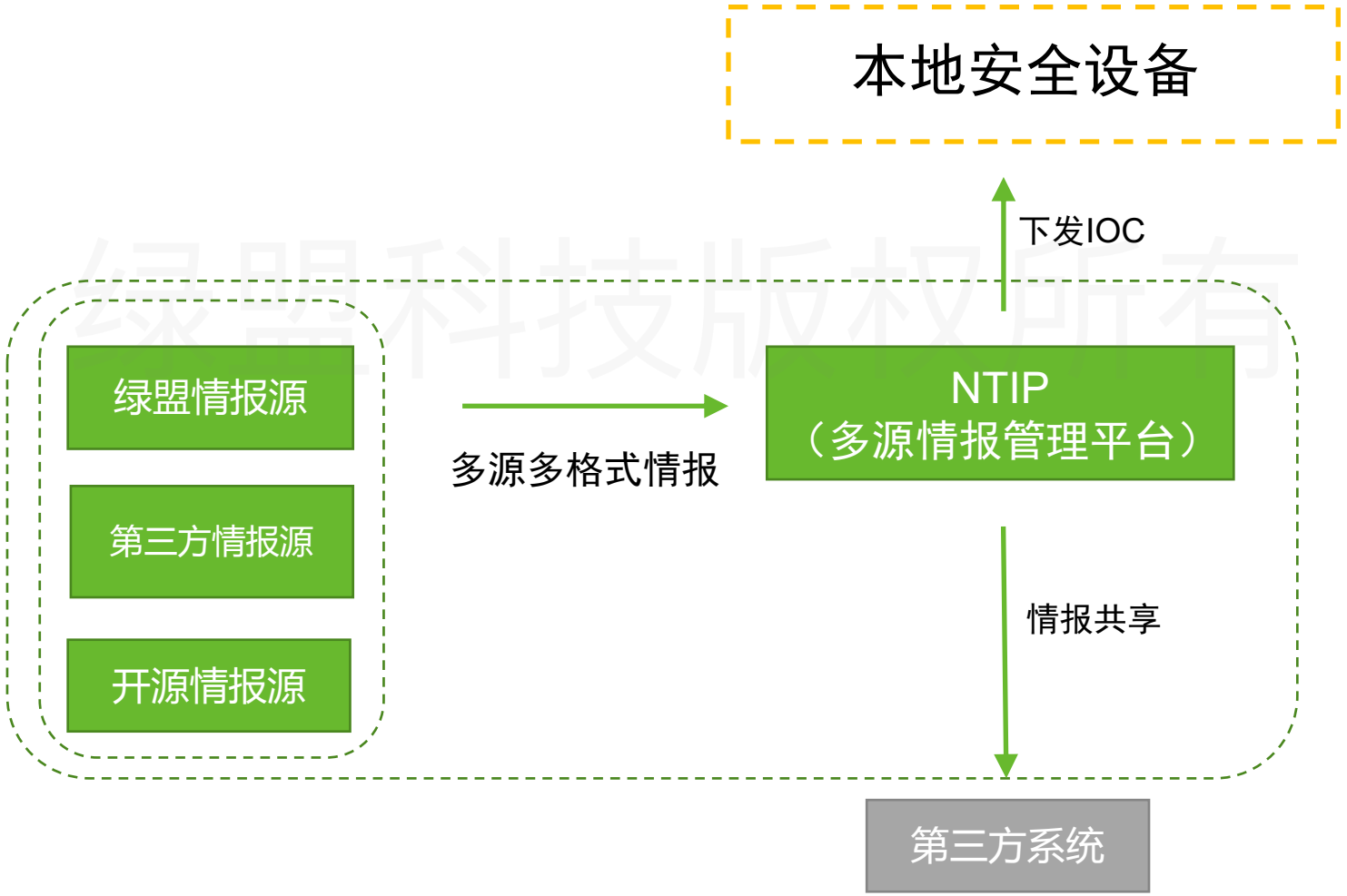
```
#!/usr/bin/env python
# -*- coding: utf-8 -*-
import urllib2
import json
import requests
import os
authkey = "xxxxxxxxxxxxxxxxxxxxx
api = "https://nti.nsfocus.com/api/v1
request = urllib2.Request(
api,
'',
{'Content-Type':'application/json',"N
)
response = urllib2.urlopen(request)
data = json.loads(response.read())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

e=all"


```
{
    "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": [ ]
    }
```


API文档

客户本地威胁情报平台（NTIP）



谢谢！

NSFOCUS